CA Process Automation

Installationshandbuch

Version 04.2.00

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden. Diese Dokumentation ist Eigentum von CA und darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, ist berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Markenzeichen, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Unternehmen.

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Änderungen in der Dokumentation

Die folgenden Dokumentationsaktualisierungen sind seit der letzten Ausgabe dieser Dokumentation vorgenommen worden:

- Was möchten Sie tun? (siehe Seite 13): Dieses vorhandene Thema wurde umbenannt und auf Links zu verschiedenen Installationsaufgaben reduziert.
- Einführung in die Komponenten eines CA Process Automation-Systems (siehe Seite 15): In diesem neuen Kapitel werden alle Komponenten beschrieben, beginnend mit jenen, die für die Einrichtung eines einfachen Systems erforderlich sind.
  - Einfaches CA Process Automation-System (siehe Seite 15)
  - Typisches CA Process Automation-System (siehe Seite 17)
  - Geclustertes CA Process Automation-System (siehe Seite 19)
  - Typische Datenbankverbindungen (siehe Seite 21)
- Die folgenden Themen wurden aktualisiert, um widerzuspiegeln, dass in Version 4.2 von CA Process Automation ausschließlich Version 1.7 von JDK unterstützt wird. Diese Voraussetzung gilt nur für Koordinationsrechner. Für Agenten unterstützt CA Process Automation Java 6-Versionen von JRE (bis JRE 1.6.0_45).
  - Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30)
  - JDK-Voraussetzungen (siehe Seite 79)
  - Datenbankhinweise zu Upgrades von CA IT PAM 2.x zu Version 4.2 von CA Process Automation.
  - Upgrade auf JDK-Version 1.7
  - Upgrade zu Version 4.2 von CA Process Automation

- Richtlinien für das Angeben des Datenbankservernamens für SQL Server (siehe Seite 77): In diesem neuen Thema wird erklärt, wie Sie eine CA Process Automation-Datenbank auf einer Instanz mit dem Namen SQL Server hosten können.
- Privilegien des Verantwortlichen für die Datenbank (siehe Seite 78): Dieses vorhandene Thema wurde korrigiert und enthält nun Informationen zu Berechtigungen für Aktionen für Ansichten.
- Installieren des Domänen-Koordinationsrechners (siehe Seite 99): Dieses vorhandene Thema wurde aktualisiert und enthält nun Informationen zu den neuen Seiten, die zum Installationsassistenten für diese Version hinzugefügt wurden.
- Interaktives Installieren eines Agenten (siehe Seite 180): Dieses vorhandene Thema wurde aktualisiert und dokumentiert nun ein neues Kontrollkästchen, über das angegeben wird, ob der Agent vereinfachte Kommunikation über standardmäßige Internet-Ports (Standard) oder veraltete Kommunikation über Port 7003 verwenden soll.
- Support nach der Installation für CA EEM-Upgrades (siehe Seite 172): In diesem neuen Thema werden Upgrades vorhandener Installationen von Version 4.2 von CA Process Automation beschrieben, wenn ein Upgrade der CA EEM-Version durchgeführt wird oder neue Zertifikate mit längeren Schlüsseln generiert werden.
- Beispielszenario: Konfigurieren der vorhandenen Installation, um CA Process Automation-Zertifikate neu zu generieren (siehe Seite 168): Dieses neue Thema gibt den Installationsvorgang an, der befolgt werden muss, wenn der CA EEM-Administrator Zertifikate mit 2048- oder 4096-Bit-Schlüsseln neu generiert, nachdem Sie CA Process Automation mit CA EEM r12.51 installiert haben.
- Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54): Dieser vorhandene Abschnitt wurde geändert. Er enthält nun Informationen zu Änderungen für die Unterstützung von vereinfachter Kommunikation, und die Verweise auf den Primärknoten wurden entfernt. Darüber hinaus wurden weitere Änderungen für verbesserte Nutzbarkeit vorgenommen.
- NGINX-Lastenausgleich (siehe Seite 35): In diesem neuen Abschnitt wird die Konfiguration des NGINX-Lastenausgleichs dokumentiert, der vereinfachte Kommunikation unterstützt. Dieser Lastenausgleich ist eine gute Alternative zu Apache, wo nur veraltete Kommunikation unterstützt wird.
- Informationen zur Agent-Kommunikation (siehe Seite 164): In diesem neuen Thema wird die neue Methode für vereinfachte Kommunikation beschrieben.

- So führen Sie ein Upgrade von CA Process Automation durch (siehe Seite 146): Dieses neue Szenario wurde zum Kapitel "Upgrade auf die aktuelle Version" hinzugefügt.
  - Durchführen von Sicherungen und Vorbereiten des Ausfalls (siehe Seite 147): Dieses neue Szenario wurde aus einem realen Kunden-Upgrade vor Ort abgeleitet.
  - Erfüllen von Upgrade-Voraussetzungen (siehe Seite 149)
  - Durchführen eines Upgrade des Domänen-Koordinationsrechners (siehe Seite 150)
  - Durchführen eines Upgrade eines nicht geclusterten Koordinationsrechners (siehe Seite 155)
  - Durchführen eines Upgrade eines Cluster-Knoten (siehe Seite 158)
  - Durchführen von Aufgaben nach dem Upgrade (siehe Seite 161): Dieses neue Thema enthält Anleitungen, die aus einem realen Kunden-Upgrade vor Ort abgeleitet wurden.
  - Testen der Prozesse mit den aktualisierten Koordinationsrechnern (siehe Seite 162)
  - Wechseln von Apache- zu NGINX-Lastenausgleich (siehe Seite 163)
  - Aktualisieren von F5-Pools, iRule-Definition und Konfiguration (siehe Seite 163)
  - Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation (siehe Seite 164)
  - Testen der Prozesse mit vereinfachter Kommunikation (siehe Seite 165)
- Upgrade-Beispiele: Dieser neue Anhang umfasst:
  - Beispiel: Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 (siehe Seite 299): Dieses neue Thema enthält spezifische Screenshots für dieses Upgrade-Szenario.
  - Beispiel: Upgrade eines Knotens des Koordinationsrechners von 3.1 SP01 auf Version 4.2 (siehe Seite 289): Dieses neue Thema enthält spezifische Screenshots für dieses Upgrade-Szenario.
  - Beispiel: Upgrade weiterer Knoten des Koordinationsrechners von 3.1 SP01 auf Version 4.2 (siehe Seite 296): Dieses neue Thema enthält spezifische Screenshots für dieses Upgrade-Szenario.
- Von CA Process Automation verwendete Ports (siehe Seite 231): In diesem neuen Anhang sind die Ports aufgelistet, die von den einzelnen Komponenten in einem typischen CA Process Automation-System verwendet werden.

Inhalt

Kapitel 1: Was möchten Sie tun? 13

Kapitel 2: Einführung in die Komponenten eines CA Process Automation-Systems 15

Einfaches CA Process Automation-System 15
Typisches CA Process Automation-System 17
Geclustertes CA Process Automation-System 19
Erweiterte Konfigurationsoptionen 21
Beispiel: So ermöglichen Kontaktpunkte die Portabilität von Inhalten 24
Herunterladen des CA Process Automation-Bookshelf ohne Internetzugriff 26

Kapitel 3: Plattformunterstützung und Hardwarevoraussetzungen 29

Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten 30
Hardwareanforderungen 32

Kapitel 4: Einrichten eines Lastenausgleichs für Koordinationsrechner-Clustering 35

NGINX-Lastenausgleich 35
- Voraussetzungen 36
- Grundlegende Kommunikation 38
- Sichere Kommunikation 43
- REST-Konfiguration 48
- Generieren von SSL-Zertifikatsdateien 51

Voraussetzungen des F5-Lastenausgleichs 54
- Erstellen eines F5-Knoten für jeden Cluster-Knoten 55
- Erstellen von zwei F5-Pools für jeden CA Process Automation-Cluster 56
- Erstellen einer F5 iRule für CA Process Automation 57
- Erstellen eines virtuellen Servers von F5 für CA Process Automation 60
- Konfigurieren von F5 für die Verwendung von vereinfachter Kommunikation mit HTTPS 62
- Vorbereiten des F5-Lastenausgleichs für die Kommunikationsüberprüfung (Beispiel) 64

Kapitel 5: Installieren des Domänen-Koordinationsrechners 67

Voraussetzungen zur Installation des Domänen-Koordinationsrechners 67
- Planen der Speicherorte für die unterstützenden Komponenten 69
- Datenbankserver-Voraussetzungen 71

JDK-Voraussetzungen 79
CA EEM-Voraussetzungen 81
Voraussetzungen für die Port-Planung 95
Interaktive Installation des Domänen-Koordinationsrechners 95
Installieren der Drittanbieter-Software 96
Installieren des Domänen-Koordinationsrechners 99
Unbeaufsichtigte Domänen-Koordinationsrechner-Installation 121
Eine Antwortdatei erstellen 121
Ausführen oder Bearbeiten der Skriptdatei für die automatische Installation 125
Hinweise zu Upgrades (automatische Installation) 127
Aufgaben nach der Installation für den Domänen-Koordinationsrechner 128
Navigieren zu CA Process Automation und Anmelden als standardmäßiger Administrator 129
Verfügbarmachen des Bookshelf für Anwender ohne Internetzugriff 132
Konfigurieren der Firewalls für bidirektionale Kommunikation 133
Installieren der Treiber für Datenbankoperatoren 134
Aktivieren der NTLM-Durchleitungs-Authentifizierung nach der Installation 135
Interaktion mit der Desktop-Konfiguration 136
Weitere Informationen finden Sie unter Konfigurieren von CA EEM, um es referenzierten Anwendern zu ermöglichen, sich mit ihrem E-Mail-Namen anzumelden 136
Voraussetzungen der Zeitsynchronisierung 138
Installieren von Patches und Connectors mit CA Process Automation 4.2 138
Ändern der Konfiguration des Oracle-Datenbankservers für die Verwendung von Oracle RAC 140
Anhalten des Koordinationsrechners 142
Starten des Koordinationsrechners 143
Deinstallieren des Domänen-Koordinationsrechners 144

Kapitel 6: Upgrade auf die aktuelle Version 145

So führen Sie ein Upgrade von CA Process Automation durch 146
Durchführen von Sicherungen und Vorbereiten des Ausfalls 147
Erfüllen von Upgrade-Voraussetzungen 149
Durchführen eines Upgrade des Domänen-Koordinationsrechners 150
Durchführen eines Upgrade eines nicht geclusterten Koordinationsrechners 155
Durchführen eines Upgrade eines Cluster-Knoten 158
Ausführen von Aufgaben nach dem Upgrade 161
Testen der Prozesse mit den aktualisierten Koordinationsrechnern 162
Wechseln von Apache- zu NGINX-Lastenausgleich 163
Aktualisieren von F5-Pools, iRule-Definition und Konfiguration 163
Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation 164
Informationen zur Agent-Kommunikation 164
Testen der Prozesse mit vereinfachter Kommunikation 165

Kapitel 7: Neuinstallation oder Konfiguration der aktuellen Version 167

Beispielszenario: Konfigurieren der vorhandenen Installation, um CA Process Automation-Zertifikate neu zu generieren 168
Support nach der Installation für CA EEM-Upgrades 172
Aktivieren der sicheren Kommunikation für ein vorhandenes CA Process Automation 176

Kapitel 8: Installieren von Agenten 177

Voraussetzungen für das Installieren von Agenten 177
- Identifizieren von Hosts, die Agenten benötigen 177
- Überprüfen der Java-Voraussetzungen für Agenten 178
- Bestimmen der Port-Verfügbarkeit für Agenten 178

Navigieren Sie zu CA Process Automation, und melden Sie sich an 179
Interaktives Installieren eines Agenten 180
Ausführen einer unbeaufsichtigten Agenteninstallation 183
Aufgaben nach der Installation für Agenten 187
- Lösen eines Port-Konflikts für einen Agenten 188
- Konfigurieren von Agenten zur Ausführung als standardmäßiger Anwender mit beschränkten Berechtigungen 189
- So starten Sie einen Agenten oder halten ihn an: 190

Kapitel 9: Hinzufügen eines Knotens zum Domänen-Koordinationsrechner 193

Voraussetzungen für das Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner 194
Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner 197
Synchronisieren der Zeit für einen Cluster-Knoten 199

Kapitel 10: Installieren von zusätzlichen Koordinationsrechnern 201

Voraussetzungen für die Installation eines Koordinationsrechners 201
Installieren eines Koordinationsrechners 204
Aufgaben nach der Installation für den Koordinationsrechner 210

Kapitel 11: Hinzufügen von Knoten zu einem zusätzlichen Koordinationsrechner 211

Voraussetzungen für das Installieren eines Cluster-Knotens für einen Koordinationsrechner 212
Installieren von Cluster-Knoten für Koordinationsrechner 215
Synchronisieren der Zeit für einen Cluster-Knoten 217

Kapitel 12: Feinabstimmung von CA Process Automation 219

So verbessern Sie die Leistung von CA Process Automation 220

Anhang A: So verwenden Sie SiteMinder mit CA Process Automation 223

CA SiteMinder-Voraussetzungen 224
Konfigurieren der Objekte von CA SiteMinder-Richtlinienservern 224
Integrieren von CA Process Automation in IIS für Single Sign-On 226
So konfigurieren Sie IIS zur Umleitung an Tomcat 227
Integrieren Sie CA Process Automation in Apachen für SSO. 229
Aktivieren der Abmeldung in CA Process Automation für SSO 230

Anhang B: Von CA Process Automation verwendete Ports 231

Kommunikation in einer typischen Architektur 232
Von CA EEM verwendete Ports 233
Vom Lastenausgleich verwendete Ports 235
Von Koordinationsrechnern verwendete Ports 238
Von Agenten verwendete Ports 249
Von Datenbankservern verwendete Ports 250
Von Web-Clients verwendete Ports 251

Anhang C: Verwalten des DNS-Namen oder der IP-Adresse des Koordinationsrechners 253

Verwalten von IP-Adressen 253
Korrigieren von ungültigen Zeichen im CA Process Automation-DNS-Namen 254
Aktivieren von DNS zur Behebung von ungültigen Hostnamen 254
Verwalten der DNS-Hostnamen 255
Syntax für DNS-Hostnamen 256

Anhang D: Fehlerbehebung 257

Fehlschlagen der CA Process Automation-Installation 257
Potenzielles Problem wenn CA Process Automation auf einem VMWare-Server mit einer E1000-Netzwerkschnittstelle ausgeführt wird 258
Oracle-Fehlernummer 9347941 260
Beschränkungen in Internet Explorer 261
CA Process Automation-Installation in Netzwerkumgebungen mit dualem Stapel (IPv4 und IPv6) 262
Unbefriedigende Leistung bei Verwendung von MySQL 262
Erstellen der Laufzeitdatenbank nicht möglich 264
Die Operatoren "Skript ausführen" und "Programm ausführen" können nicht auf RHEL6 ausgeführt werden 265

Anhang E: Apache-Lastenausgleich 267

Voraussetzungen des Apache-Lastenausgleichs 267

Apache-Lastenausgleichs-Konfiguration unter Windows 267
Grundlegende Konfiguration (Windows) 268
Sichere Konfiguration (Windows) 272
Apache-Lastenausgleichs-Konfiguration unter Nicht-Windows-Betriebssystemen 278
Grundlegende Konfiguration (Nicht-Windows-Betriebssystem) 279
Konfigurieren der sicheren Konfiguration (Nicht-Windows-Betriebssystem) 283

Anhang F: Upgrade-Beispiele 289

Beispiel: Upgrade eines Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows 289
Beispiel: Upgrade eines weiteren Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows 296
Beispiel: Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 unter Windows 299
Upgrade von Versionen vor 3.1 SP01 305

Kapitel 1: Was möchten Sie tun?

- **Erstinstallation von CA Process Automation**
  - Einführung in die Komponenten eines CA Process Automation-Systems (siehe Seite 15).
  - Plattformunterstützung und Hardwarevoraussetzungen (siehe Seite 29).
  - Installieren des Domänen-Koordinationsrechners (siehe Seite 67).
- **Upgrade von einer früheren Version von CA Process Automation** (siehe Seite 145)
- Aktualisieren der aktuellen CA Process Automation-Version, um folgende Aktionen durchführen zu können:
  - Verwenden mehrerer Active Directory-Domänen. (siehe Seite 172) (nach einem Upgrade von CA EEM auf 12.5)
  - Verwenden der neuen Zertifikate von CA EEM 12.5 (siehe Seite 168) (bei einer vorhandenen Installation von CA EEM 12.5)
  - Aktivieren von sicherer Kommunikation (HTTPS) (siehe Seite 176)
  - Verwenden einer neuen Host-IP-Adresse (siehe Seite 253)
- Installieren eines Agenten (siehe Seite 177).
- Systemausbau
  - Einrichten eines Lastenausgleichs für Koordinationsrechner-Clustering (siehe Seite 35)
  - Hinzufügen eines Knotens zum Domänen-Koordinationsrechner (siehe Seite 193).
  - Installieren eines zusätzlichen Koordinationsrechners (siehe Seite 201).
  - Hinzufügen eines Knotens zu einem zusätzlichen Koordinationsrechner (siehe Seite 211).
- Fehlerbehebung (siehe Seite 257)
- CA SiteMinder mit CA Process Automation verwenden (siehe Seite 223)

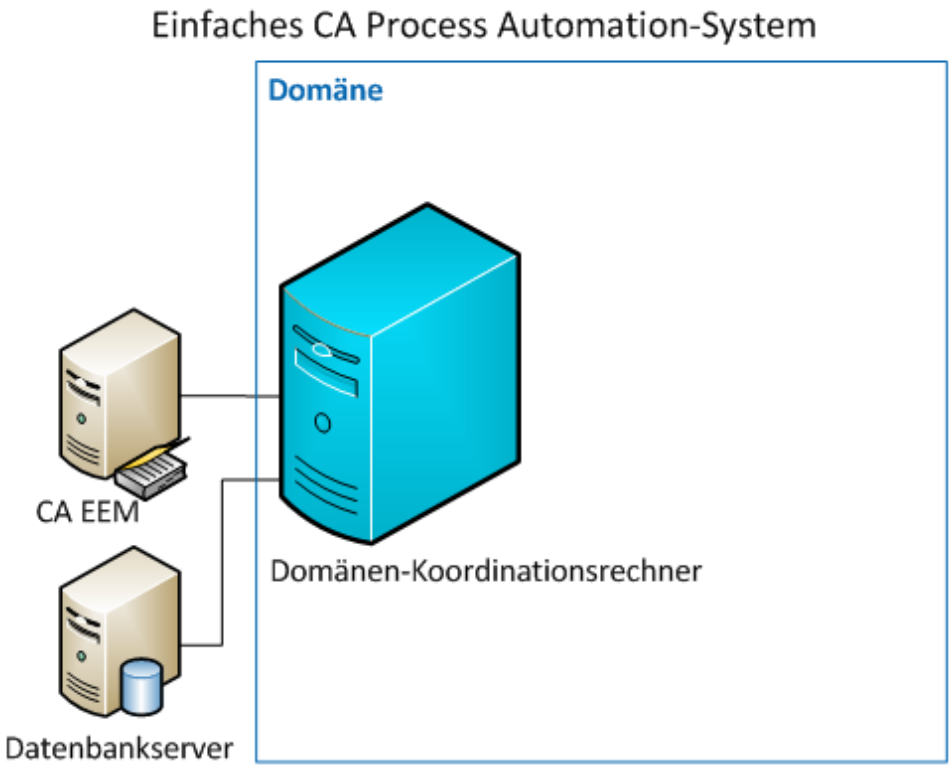
Kapitel 2: Einführung in die Komponenten eines CA Process Automation-Systems

Dieses Kapitel enthält folgende Themen:

Einfaches CA Process Automation-System (siehe Seite 15)
Typisches CA Process Automation-System (siehe Seite 17)
Geclustertes CA Process Automation-System (siehe Seite 19)
Erweiterte Konfigurationsoptionen (siehe Seite 21)
Beispiel: So ermöglichen Kontaktpunkte die Portabilität von Inhalten (siehe Seite 24)
Herunterladen des CA Process Automation-Bookshelf ohne Internetzugriff (siehe Seite 26)

Einfaches CA Process Automation-System

Ein einfaches CA Process Automation-System enthält drei Komponenten: Domänen-Koordinationsrechner, Datenbankserver und eine Instanz von CA Embedded Entitlements Manager (CA EEM).



Domänen-Koordinationsrechner

Koordinationsrechner sind CA Process Automation-Server. Anwender stellen eine Verbindung mit einem Koordinationsrechner her, um Prozesse zu entwerfen und zu testen, Prozesse auszuführen und das CA Process Automation-System auf verschiedenen Arten zu konfigurieren. Jedes CA Process Automation-System hat einen Domänen-Koordinationsrechner und kann über einen oder mehrere Koordinationsrechner verfügen, die keine Domänen-Koordinationsrechner sind. Eine einfache Bereitstellung verwendet einen einzigen Domänen-Koordinationsrechner.

Datenbankserver

Im Zuge der Installation des Domänen-Koordinationsrechners identifizieren Sie den Datenbankserver, in dem die drei CA Process Automation-Datenbanken erstellt werden sollen.

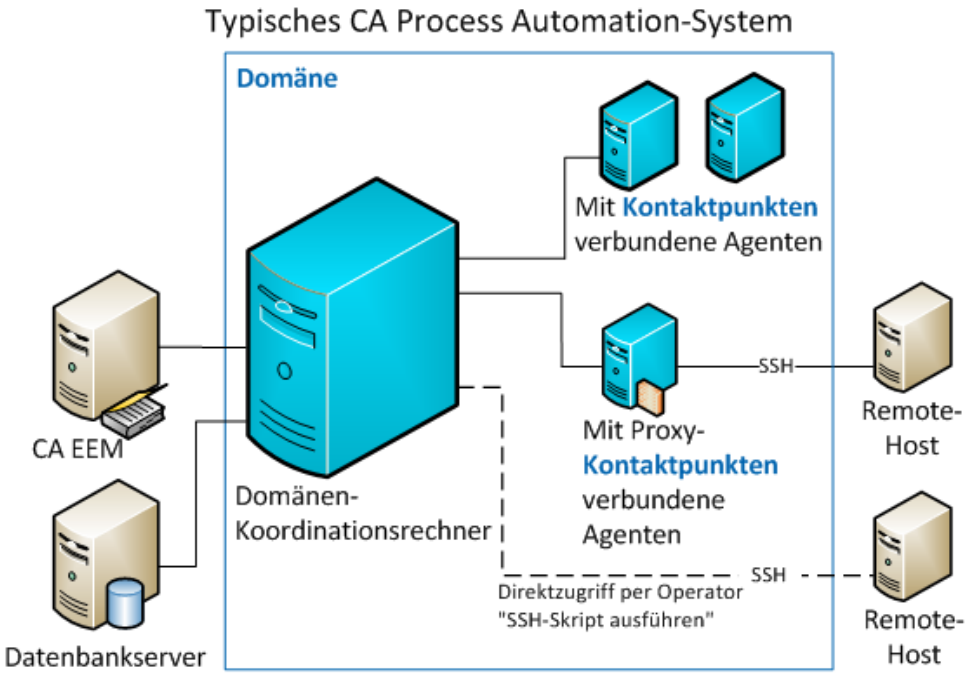
- In der Bibliotheksdatenbank wird der Automatisierungsinhalt, den Sie erstellen, gespeichert. Beispiele umfassen Prozesse, Datensätze und Formulare.
- In der Laufzeitdatenbank werden Zustandsinformationen zu Prozessinstanzen, die ausgeführt wurden oder derzeit ausgeführt werden, gespeichert.
- In der Berichtsdatenbank werden Informationen zu Prozessinstanzen gespeichert, die in einem Format, das sich für die Berichterstellung eignet, ausgeführt wurden.

CA Embedded Entitlements Manager (CA EEM)

- Im Zuge der Installation des Domänen-Koordinationsrechners registrieren Sie die CA Process Automation-Anwendung mit CA EEM. Eine Instanz von CA EEM kann für mehrere CA Technologies-Produkte verwendet werden, damit Anwenderidentitäten und die dazugehörigen Anwendungsberechtigungen zusammengefasst verwaltet werden können.
- CA Process Automation-Anwender werden von CA EEM authentifiziert. CA EEM versucht, die Anmeldeinformationen, die von Anwendern angegeben werden, mit Anmeldeinformationen von bekannten CA Process Automation-Anwendern abzugleichen. Die gültigen Anmeldeinformationen können direkt in CA EEM erstellt werden. Häufiger wird jedoch aus einem oder mehreren LDAP-basierten Repositorys wie Microsoft Active Directory von CA EEM auf sie verwiesen.
- Die Autorisierungsebenen für CA Process Automation-Anwender werden ebenfalls von CA EEM verwaltet. Nach der Installation von CA Process Automation weisen Sie in CA EEM zu den einzelnen Anwenderkonten Berechtigungen zu, um den Anwendern die jeweils passenden Berechtigungen in der CA Process Automation-Anwendung zu erteilen.

Typisches CA Process Automation-System

In vielen Bereitstellungen ist es erforderlich, dass ein Teil Auslastung auf Hosts, bei denen es sich nicht um den Domänen-Koordinationsrechner handelt, umverteilt werden kann. Bestimmte Auslastungsarten können auf Remote-Hosts ohne installierte Agenten ausgeführt werden. Es sind jedoch mehr Funktionen verfügbar, wenn auf dem Zielhost ein CA Process Automation-Agent installiert ist.



Agenten

Jede Prozessinstanz besteht aus einem oder mehreren Operatoren. Jeder Operator ist für die Ausführung auf einem spezifischen Host bestimmt. Diese kann direkt oder indirekt unter Verwendung von Kontaktpunkten erfolgen. Jeder Kontaktpunkt ist über die Systemkonfiguration zu einem spezifischen Host zugeordnet.

Ein Kontaktpunktname kann zu unterschiedlichen Hosts in verschiedenen CA Process Automation-Domänen oder -Umgebungen zugeordnet sein. Dadurch ermöglichen es Kontaktpunkte, denselben Prozessinhalt unverändert in verschiedenen CA Process Automation-Domänen oder -Umgebungen bereitzustellen.

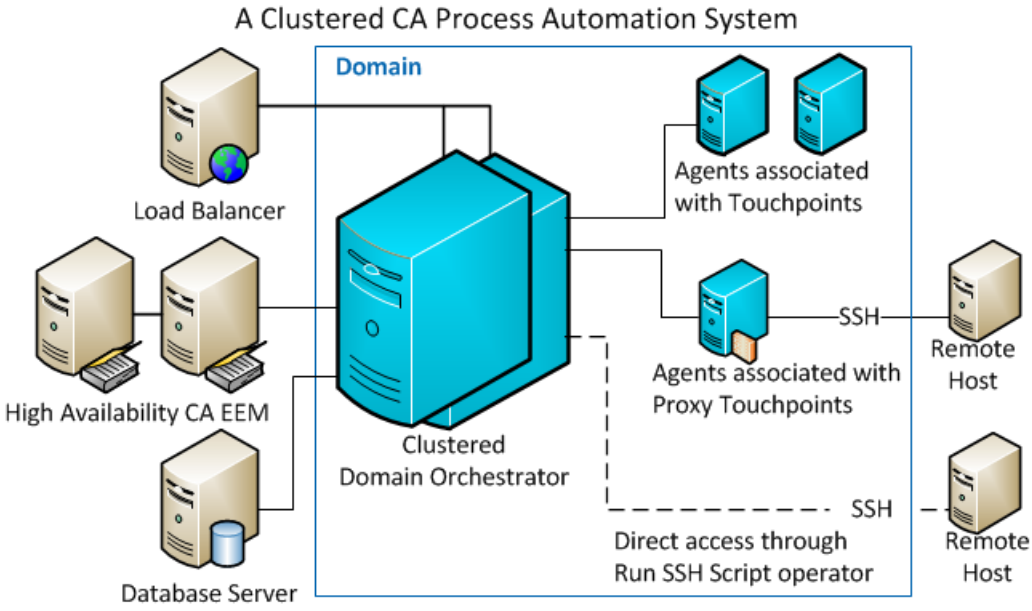
Kontaktpunkte können zu einem CA Process Automation-Koordinationsrechner oder einem CA Process Automation-Agenten zugeordnet sein. Proxy-Kontaktpunkte sind zu Remote-Hosts ohne installierter CA Process Automation-Software zugeordnet. Koordinationsrechner können Auslastung auf einen Remote-Host umverteilen, indem sie direkt über SSH eine Verbindung mit diesem Remote-Host herstellen oder sich über einen Agent, welcher wiederum eine SSH-Verbindung mit dem Remote-Host verwendet, mit ihm verbinden.

Wie Kontaktpunkte sind auch Proxy-Kontaktpunkte logische Entitäten. Es handelt sich um einen Namen, der im Prozessdesigner verwendet werden kann, um ein Ausführungsziel für einen Operator anzugeben. Während ein Kontaktpunkt über die Umgebungskonfiguration definiert und einem bestimmten Agenten zugeordnet ist, ist ein Proxy-Kontaktpunkt einem spezifischen agentenlosen Remote-Host zugeordnet. Agentenlose (zu einem Proxy-Kontaktpunkt zugeordnete) Remote-Hosts werden von Agenten verwaltet, die jeweils auf unterschiedlichen Hosts installiert sind. Wenn ein Koordinationsrechner Arbeitsschritte verteilt, deren Ziel ein Proxy-Kontaktpunkt ist, werden sie an den Agenten gesendet, der den Remote-Host verwaltet und wiederum eine SSH-Verbindung mit dem Remote-Host aufbaut, um die Arbeit auszuführen.

Die Hauptaufgabe eines CA Process Automation-Agenten besteht folglich darin, Arbeitsschritte auf dem Host auszuführen, auf dem er installiert ist. Zusätzlich können Agenten als Gateway agieren, über das Auslastung auf Remote-Hosts verteilt wird, auf denen Sie keinen Agenten installieren können.

Geclustertes CA Process Automation-System

In vielen Installationen wird ein geclusterter Domänen-Koordinationsrechner bereitgestellt, um die Hochverfügbarkeit und Skalierbarkeit der Bereitstellung zu gewährleisten.



Geclusterte Koordinationsrechner

Ein geclusterter Koordinationsrechner besteht aus mindestens zwei Knoten. In normalen Vorgängen wird die Auslastung über den Knoten des Koordinationsrechners aufgeteilt. Zusätzliche Knoten können hinzugefügt werden, um die Kapazität des Koordinationsrechners bedarfsgerecht zu skalieren. Wenn ein Koordinationsrechner-Knoten fehlschlägt, übernehmen die anderen Knoten bis zu dessen Wiederherstellung die Aufgaben des fehlgeschlagenen Knotens, wodurch Hochverfügbarkeit gegeben ist.

Jeder Koordinationsrechner wird auf einem separaten Host installiert. Installation und Upgrades werden für jeden Knoten separat durchgeführt.

Hinweis: Wenn Sie einen Koordinationsrechner zuvor in einer eigenständigen Konfiguration installiert hatten, müssen Sie den Installationsassistenten erneut ausführen, um ihn als Knoten eines geclusterten Koordinationsrechners neu zu konfigurieren.

Lastenausgleich

CA Process Automation unterstützt sowohl hardwarebasierte als auch softwarebasierte Lastenausgleiche, zum Beispiel:

- F5
- NGINX
- Apache (mit funktionellen Einschränkungen)

Hinweis: Der Apache-Lastenausgleich wird für die Kommunikation zwischen Agenten, für die ein Upgrade durchgeführt wurde, und einem geclusterten Koordinationsrechner unterstützt. Das Protokoll, das für den vereinfachten Kommunikationsmechanismus benötigt wird, wird vom Apache-Lastenausgleich jedoch nicht unterstützt. Sie können das veraltete Kommunikationsmodell weiterhin mit Apache verwenden. Wenn Sie eine Bereitstellung mit einem softwarebasierten Lastenausgleich planen, wird jedoch nachdrücklich empfohlen, NGINX zu verwenden.

CA EEM mit Hochverfügbarkeit

Für Bereitstellungen, die eine vollständige Hochverfügbarkeitskonfiguration benötigen, kann CA EEM mit einem Failover-Knoten konfiguriert werden.

Erweiterte Konfigurationsoptionen

Nicht-Domänen-Koordinationsrechner

Sie können die Automatisierungsauslastung aufteilen, indem Sie weitere Koordinationsrechner bereitstellen. Wie Domänen-Koordinationsrechner können auch diese Koordinationsrechner, die keine Domänen-Koordinationsrechner sind, geclustert werden.

Es kann vorkommen, dass bestimmte Arbeitsschritte in einem spezifischen Datencenter oder einer bestimmten geografischen Region ausgeführt werden müssen und das CA Process Automation-System an den einzelnen Standorten unterschiedlich konfiguriert sein muss. Ein möglicher Ansatz besteht darin, in jedem Datencenter einen Koordinationsrechner bereitzustellen und Konfigurationsvorgänge auf Koordinationsrechnerebene zu verwenden, um die Konfiguration auf Domänenebene bedarfsgemäß zu überschreiben.

Umgebungen

Eine standardmäßige Bereitstellung umfasst eine Domäne und eine Umgebung, die Standardumgebung.

Sie können eine CA Process Automation-Domäne in mehrere Umgebungen aufteilen. Dadurch können verschiedene Aspekte der Domänenkonfiguration für die Erfordernisse der einzelnen Umgebungen angepasst werden. Wenn Sie mehrere Umgebungen verwenden, können Sie beispielsweise Entwicklungsumgebungen anders konfigurieren als Test- oder Produktionsumgebungen.

Jede Umgebung kann über eine eigene Bibliothek verfügen, sodass die Inhaltsversionen in den unterschiedlichen Umgebungen möglicherweise voneinander abweichen.

Durch Umgebungen wird auch die Auslastung aufgeteilt. Alle Koordinationsrechner werden zu einer Umgebung zugeordnet. Die Standardumgebung enthält den Domänen-Koordinationsrechner und kann über einen oder mehrere Koordinationsrechner, die keine Domänen-Koordinationsrechner sind, verfügen. Alle anderen Umgebungen haben einen oder mehrere Koordinationsrechner, die keine Domänen-Koordinationsrechner sind. Alle Domänen-Koordinationsrechner und alle Nicht-Domänen-Koordinationsrechner können geclustert (mehrere Knoten) oder nicht geclustert (ein Knoten) sein.

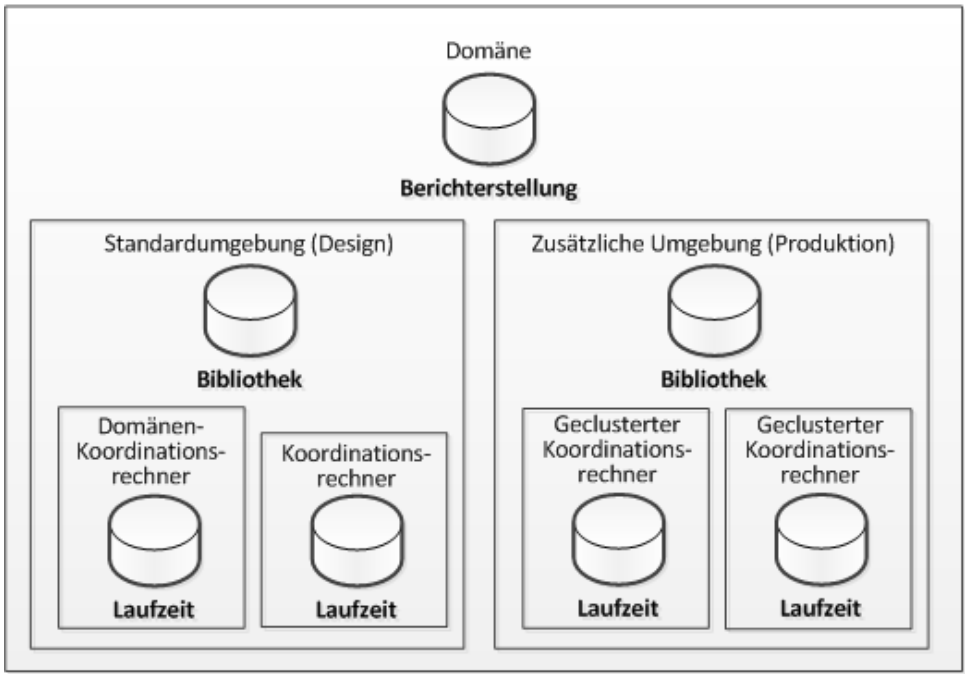
Umgebungen können Ihnen auch dabei helfen, die Auslastung innerhalb eines Produktionskontexts aufzuteilen. Zum Beispiel kann ein Service Provider eine Umgebung je Kunde bereitstellen. Diese Einrichtung ermöglicht es Ihnen, denselben standardmäßigen Automatisierungsinhalt in mehreren Umgebungen, deren Auslastung physisch aufgeteilt ist, auszuführen. Diese Umgebungen, in denen derselbe Inhalt ausgeführt wird, sind unterschiedlich konfiguriert und werden möglicherweise an unterschiedlichen geografischen Standorten ausgeführt.

Auswirkungen des Hinzufügens von Umgebungen und Nicht-Domänen-Koordinationsrechnern auf Datenbanken

Bezüglich der gemeinsamen Verwendung von Datenbanken in mehreren Koordinationsrechnern besteht Flexibilität. Gebräuchliche Zuordnungen sind:

- Eine Berichtsdatenbank, die von allen Koordinationsrechnern in der Domäne genutzt wird. Datenbanken können nicht domänenübergreifend verwendet werden, doch es besteht die Möglichkeit, mehr als eine Berichtsdatenbank zu verwenden.
- Eine Bibliotheksdatenbank je Umgebung, wobei jede Bibliotheksdatenbank von allen Koordinationsrechnern in der Umgebung genutzt wird.
- Eine Laufzeitdatenbank je Koordinationsrechner. Dies ist erforderlich. Jeder eigenständige (nicht geclusterte) Koordinationsrechner verfügt über eine eigene Laufzeitdatenbank. Jeder geclusterte Koordinationsrechner verwendet eine einzige Laufzeitdatenbank.

Typische Datenbankverbindungen



In einer einfachen Bereitstellung mit einem nicht geclusterten Domänen-Koordinationsrechner in der Standardumgebung werden die drei CA Process Automation-Datenbanken auf einem Datenbankserver installiert.

Das Hinzufügen weiterer Umgebungen und die Installation von Koordinationsrechnern, die keine Domänen-Koordinationsrechner sind, erhöht die Komplexität der erforderlichen Datenbankkonfiguration signifikant.

Weitere Informationen:

Informationen zu CA Process Automation-Datenbanken (siehe Seite 72)

Beispiel: So ermöglichen Kontaktpunkte die Portabilität von Inhalten

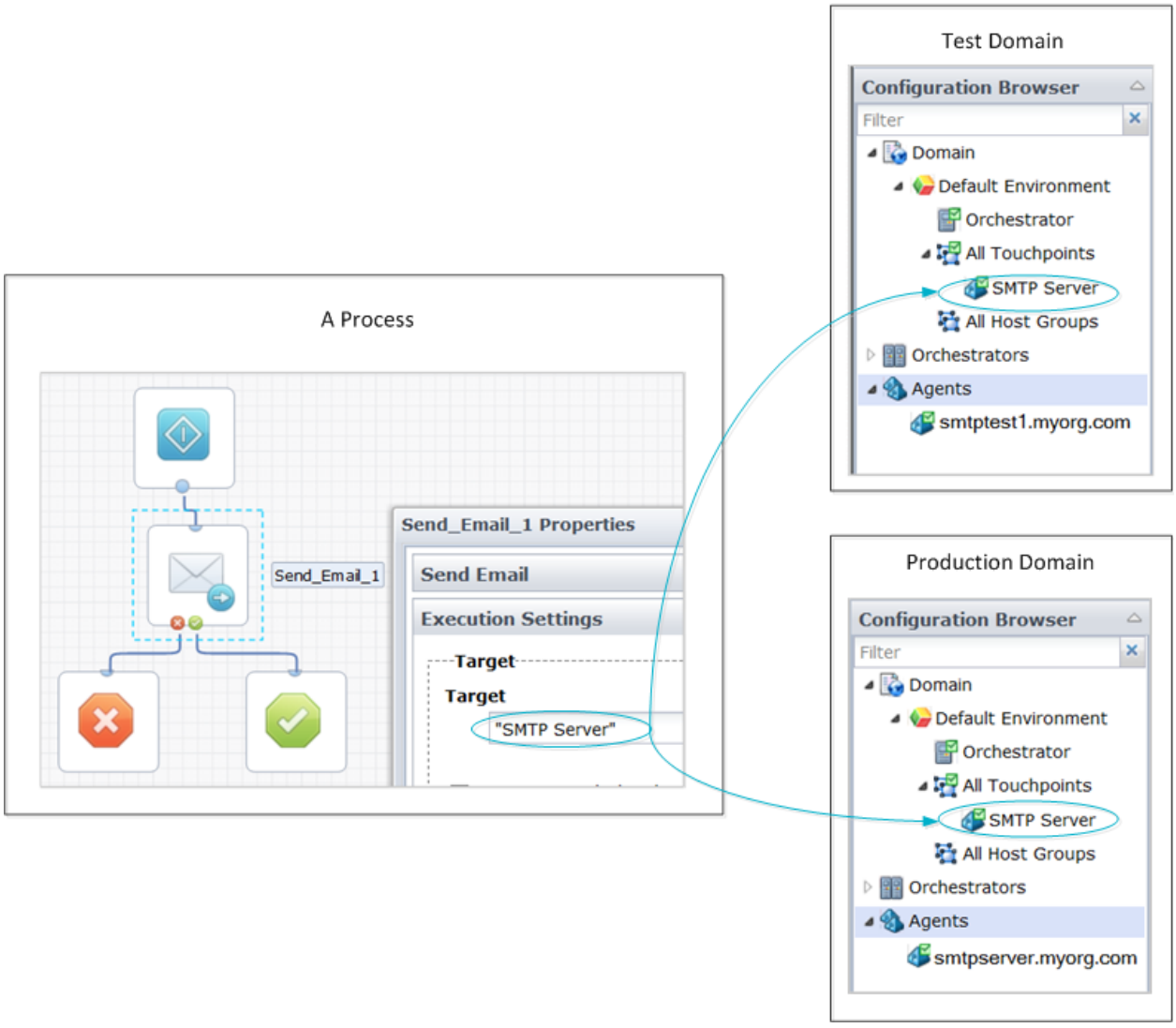
Eine Bereitstellung kann beispielsweise eine Testdomäne und eine Produktionsdomäne umfassen, die jeweils über einen eigenen SMTP-Server verfügen.

- smtptest1.myorg.com in der Testdomäne
- smptserver.myorg.com in der Produktionsdomäne

Der Administrator installiert auf jedem SMTP-Server einen Agenten und konfiguriert die Agenten jeweils mit einem Kontaktpunkt namens "SMTP-Server". Ein Inhaltsdesigner erstellt einen Prozess mit einem Send_Email-Operator, als dessen Ausführungsziel der Kontaktpunktname **SMTP-Server** festgelegt wird. Dieser Prozess kann ohne Änderungen an Testdomäne und Produktionsdomäne bereitgestellt werden.

Hinweis: In den CA Process Automation-Handbüchern und der Online-Hilfe wird beschrieben, wie Sie die Portabilität von Inhalten für mehrere Umgebungen innerhalb einer einzelnen Domäne einrichten können.

Ein Prozess kann unverändert in mehreren Bereitstellungsumgebungen bereitgestellt werden



Herunterladen des CA Process Automation-Bookshelf ohne Internetzugriff

In diesem Abschnitt wird beschrieben, wie das CA Process Automation-Bookshelf ohne Internetzugriff heruntergeladen werden kann.

Hinweis: Um auf das CA Process Automation-Bookshelf zugreifen zu können, müssen Sie die Datei *bookshelf.zip* auf alle CA Process Automation-Knoten herunterladen.

Gehen Sie folgendermaßen vor:

1. Verwenden Sie die Administrator-Anmeldeinformationen, um sich bei einem CA Process Automation-Knoten mit Internetzugriff anzumelden.

   Die CA Process Automation-Benutzeroberfläche wird geöffnet.

2. Klicken Sie auf der CA Process Automation-Benutzeroberfläche im Drop-down-Feld "Hilfe" auf den Link "Bookshelf".

   Das CA Process Automation-Bookshelf wird geöffnet.

3. Klicken Sie auf der Seite mit dem CA Process Automation-Bookshelf auf den Link *Download this Bookshelf* (Dieses Bookshelf herunterladen).

   Es wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, die ZIP-Datei zu speichern.

4. Erstellen Sie unter dem folgenden Verzeichnis einen Ordner namens *bookshelf*:

   <Server_Speicherort>\c2o\.c2orepository\

5. Erstellen Sie einen *<Gebietsschema-Ordnernamen>* für die Bookshelf-Sprache, die am folgenden Speicherort ausgewählt wird:

   <Server_Speicherort>\c2o\.c2orepository\bookshelf\

   Hinweis: Verwenden Sie den korrekten *<Gebietsschema-Ordnernamen>* für die ausgewählte Bookshelf-Sprache:

   - Englisch: *<Gebietsschema-Ordnername>* ist *en_US*
   - Deutsch: *de_DE*
   - Spanisch: es_ES
   - Französisch: *fr_FR*
   - Italienisch: *it_IT*
   - Japanisch: *ja_JP*
   - Portugiesisch: *pt_BR*
   - Türkisch: *tr_TR*
   - Chinesisch: *zh_CN*

6. Dekomprimieren Sie die ZIP-Datei, und stellen Sie die CA Process Automation-Bookshelf-Dateien in den folgenden lokalen Ordner:

   <*Server_Speicherort*>\c2o\.c2orepository\bookshelf\<*Gebietsschema-Ordnername*>\Bookshelf-Dateien.

   Jetzt können Sie vom lokalen Ordner auf die CA Process Automation-Bookshelf-Dateien zugreifen.

Kapitel 3: Plattformunterstützung und Hardwarevoraussetzungen

Dieses Kapitel enthält folgende Themen:

Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30)
Hardwareanforderungen (siehe Seite 32)

Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten

Folgende Tabelle fasst die Plattformen zusammen, die CA Process Automation-Komponenten unterstützten.

Hinweis: Das aufgelistete Betriebssystem und die Software-Unterstützung können sich im Laufe der Zeit ändern. Aktuelle Informationen zur Versionsunterstützung finden Sie auf "support.ca.com" unter "Compatibilities" (Kompatibilitäten).

CA Process Automation-Komponente	Unterstützte Betriebssysteme	Benötigte Software	Weitere Anforderungen
Koordinationsrechner	Microsoft Windows Server 2003 R2 x64 SPx, 2008 x64 SPx, 2012 x64 Solaris SPARC 10 Solaris 11 Red Hat Enterprise Linux 5 x64, 6 x64 SPx CentOS Linux 6 x64	Java Development Kit (JDK) 1.7 **Hinweis:** JDK 1.7 wird auch von Version 3.4 des eingebetteten Catalyst benötigt. Catalyst unterstützt die REST API und alle UCF-Connectors.	Weitere Informationen finden Sie in Voraussetzungen für die Installation des Domänen-Koordinationsrechners (siehe Seite 67).

CA Process Automation-Komponente	Unterstützte Betriebssysteme	Benötigte Software	Weitere Anforderungen
Agent	Microsoft Windows Server 2003 R2 x64 SPx, 2003 R2 x32 SPx, 2008 x64 SPx, 2012 x64 SUSE Linux Enterprise Server 10 x64,11 x32 SPx, 11 x64 SPx Solaris SPARC 9, 10 Solaris 10 x86 x32 Bit, 11 Red Hat Enterprise Linux 5 x64, 6 x32 SPx, 6 x64 SPx CentOS Linux 6 x64 AIX 6.1, 7.1 HP-UX 11i V3 (Itanium)	Eine der folgenden Versionen von Java Runtime Environment (JRE), das vom Betriebssystem unterstützt wird. ■ Für Windows, Solaris SPARC und Linux: Oracle JRE 1.6 und 1.7. ■ Für AIX, IBM JRE 1.6 ■ Für HP-UX lautet die minimale Ebene 1.6_04. HP Java 1.6 (JRE). **Wichtig!** Verwenden Sie nicht die Aktualisierungen 27 (1.6.0_27) bis 29 (1.6.0_29) von Java 6 Runtime Environment. Ein Problem mit diesen Versionen wirkt sich auf Anwendungen einschließlich CA Process Automation aus, die für die Verbindung mit Microsoft SQL Server JDBC verwenden. Die SDN-Fehlerdatenbank listet diesen Fehler als Fehler 7105007 auf. Java 1.6 Aktualisierung 45 ist die höchste Java 6-Version, die von CA Process Automation-Agenten unterstützt wird.	Für Proxy-Kontaktpunkte und Hostgruppen muss jeder Remote-Host einen SSHv2-Server ausführen. Ein UNIX-Remote-Host muss über "ksh" verfügen.
Datenbankserver	Weitere Informationen zu unterstützten Betriebssystemen finden Sie in der Dokumentation des Anbieters.	Eine der folgenden relationalen Datenbanken: ■ MySQL r5.5 ■ Microsoft SQL Server 2005, 2008, 2008 R2, 2012 ■ Oracle 11g R2	Detaillierte Informationen zu den Voraussetzungen finden Sie unter Datenbankserver-Voraussetzungen (siehe Seite 71). Für Oracle empfehlen wir 11.1.0.7 oder 11.2.0.2 oder höher.

CA Process Automation-Komponente	Unterstützte Betriebssysteme	Benötigte Software	Weitere Anforderungen
Verzeichnisserver	Weitere Informationen finden Sie in der Dokumentation von CA Embedded Entitlements Manager (CA EEM).	CA Embedded Entitlements Manager (CA EEM) r8.4 SP4 oder CA EEM r12.0 bis r12.51.	
Browserbasierte Anwenderoberfläche	N. rel.	Einer der folgenden Browser: ■ Microsoft Internet Explorer 9x, 10 ■ Google Chrome, Version 17, 18 ■ Mozilla Firefox 4.*x* bis 15.0 ■ Apple Safari **Hinweis:** Wenn Sie Firefox oder Chrome verwenden, deaktivieren Sie die Inline-Rechtschreibprüfung, um unnötige Verarbeitung zu vermeiden.	JavaScript aktiviert Adobe Flash Player

Hardwareanforderungen

In der folgenden Tabelle sind die Mindest-Hardwareanforderungen für die einzelnen CA Process Automation-Komponenten aufgelistet:

CA Process Automation-Komponente	Benötigte Hardware
Koordinationsrechner	■ Serverhardware mit mehreren CPUs oder CPUs mit Mehrkernprozessoren ■ 8 GB RAM ■ 40 GB freier Festplattenspeicher ■ Netzwerkverbindung mit 100 MBit/s **Hinweis:** Wir empfehlen 1000 MBit/s.
Agent	■ Host, auf dem ein unterstütztes Betriebssystem ausgeführt werden kann ■ 2 GB RAM ■ 4 GB Festplattenspeicher ■ Netzwerkverbindung mit 100 MBit/s

CA Process Automation-Komponente	Benötigte Hardware
Datenbankserver	Siehe Spezifikationen des Anbieters. Zusätzlicher Speicher, der für die Datenbanken, die gehostet werden, erforderlich ist. **Hinweis:** Wir empfehlen mindestens 40 GB für Ihre Datenbanken.
CA EEM	Lesen Sie die CA Embedded Entitlements Manager-Dokumentation.
Browserbasierte Anwenderoberfläche	Ein beliebiger Host, der einen unterstützten Browser ausführen kann.

Hinweis: Die Konfigurationen könnten für physische und für virtuelle Rechner vorgesehen sein.

Kapitel 4: Einrichten eines Lastenausgleichs für Koordinationsrechner-Clustering

Es wird nachdrücklich empfohlen, Ihre Apache-Lastenausgleichssoftware durch einen NGINX-Lastenausgleich zu ersetzen. NGINX ermöglicht vereinfachte Kommunikation zwischen Agenten und Koordinationsrechnern. Apache unterstützt nur veraltete Kommunikation.

Wenn Sie einen Koordinationsrechner zu einem späteren Zeitpunkt möchten, richten Sie einen Lastenausgleich ein, bevor Sie den Koordinationsrechner installieren, und konfigurieren Sie den Koordinationsrechner als node1.

Der Prozess für NGINX ähnelt jenem für Apache:

1. Installieren eines Lastenausgleichs.
2. Konfigurieren der einfachen Kommunikation.
3. Installieren von CA Process Automation einschließlich Cluster-Knoten.
4. Generieren der SSL-Zertifikatsdateien.
5. Konfigurieren der sicheren Kommunikation.

Dieses Kapitel enthält folgende Themen:

NGINX-Lastenausgleich (siehe Seite 35)
Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54)

NGINX-Lastenausgleich

Ein *geclusterter Koordinationsrechner* ist ein Satz an Knoten, die angezeigt werden und als ein allein stehender Koordinationsrechner agieren und eine gemeinschaftlich genutzte Bibliothek verwenden. Sie können einen CA Process Automation-Koordinationsrechner für Hochverfügbarkeit, Fehlertoleranz und Skalierbarkeit clustern.

Ein Lastenausgleich, wie z. B. der NGINX-HTTP-Server, ist für das Clustering eines Koordinationsrechners, einschließlich des Domänen-Koordinationsrechners, erforderlich. Ein Lastenausgleich ist kein Teil der CA Process Automation-Installation. Sie müssen einen Lastenausgleich installieren und konfigurieren, bevor Sie CA Process Automation installieren.

Der vereinfachte Kommunikationsmodus, der in CA Process Automation 4.2 eingeführt wird, verwendet Web-Sockets und HTTP, um eine unidirektionale, persistente Verbindung vom Agenten zum Koordinationsrechner herzustellen. CA Technologies unterstützt NGINX für diese neue vereinfachte Kommunikationsmethode. Sie können jedoch einen beliebigen Lastenausgleich verwenden, der Web-Sockets unterstützt.

Hinweis: Der Apache-Lastenausgleich unterstützt den neuen vereinfachten Kommunikationsmodus für Agenten *nicht*. Verwenden Sie NGINX oder einen anderen Web-Socket-basierten Lastenausgleich, um diese Funktion zu nutzen. Wenn Sie den vereinfachten Kommunikationsmodus nicht verwenden und die veraltete Kommunikationsmethode verwenden möchten, können Sie den Apache-Lastenausgleich installieren.

Installieren Sie den NGINX-Lastenausgleich auf einem Host außerhalb von CA Process Automation, um die Kompatibilität der Betriebssysteme sicherzustellen. Weitere Informationen zu unterstützten Betriebssystemen finden Sie in der NGINX-Dokumentation.

Ein Lastenausgleich wird *nur* für einen Koordinationsrechner in einer geclusterten Konfiguration und in bestimmten Single-Sign-On-Konfigurationen (SSO) erforderlich.

Wichtig! Wenn Sie einen vorhandenen eigenständigen Koordinationsrechner clustern möchten, installieren und konfigurieren Sie einen Lastenausgleich, und installieren Sie den Koordinationsrechner anschließend neu.

Voraussetzungen

Nachstehend finden Sie die Voraussetzungen für die Verwendung des NGINX-Lastenausgleichs.

NGINX installieren

NGINX ist eine freie Open Source-Webserversoftware, die Sie für Ihr Betriebssystem herunterladen und installieren können. CA Process Automation wurde mit Version 1.4.2 von NGINX zertifiziert. Befolgen Sie als erste Schritte die folgenden Anweisungen.

Windows

Laden Sie das NGINX-Paket herunter, und extrahieren Sie die Dateien.

Linux

Gehen Sie folgendermaßen vor:

1. Laden Sie das NGINX-Paket herunter, und extrahieren Sie die Dateien.
2. Öffnen Sie eine Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um NGINX zu installieren:

```
rpm -ivh nginx-release-rhel-6-0.el6.ngx.noarch.rpm
wget
http://nginx.org/packages/rhel/6/noarch/RPMS/nginx-release-
rhel-6-0.el6.ngx.noarch.rpm
yum install nginx
```

Hinweis: Die zuvor aufgelisteten Befehle gelten für Red Hat Enterprise Linux. Für die Äquivalente dieser Befehle für andere Linux-Versionen lesen die BS- und NGINX-Dokumentation.

Rufen Sie NGINX sowohl unter Windows als auch unter Linux über einer Eingabeaufforderung auf. Navigieren Sie zum NGINX-Verzeichnis, und geben Sie Folgendes ein:

```
nginx.exe
```

Um sicherzustellen, dass NGINX erfolgreich installiert wurde und ausgeführt wird, greifen Sie über einen Browser auf die URL zu:

http://*hostname*:80

Kopieren der Konfigurationsvorlagen

Nachdem NGINX installiert wurde, extrahieren Sie die Vorlagedateien aus den CA Process Automation-Installationsdatenträgern in Ihr NGINX-Installationsverzeichnis.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zum folgenden Ordner auf dem CA Process Automation-Installationsdatenträger:

   Installationsverzeichnis/DVD1/NginxConfTemplates

2. Extrahieren Sie die Dateien aus "NginxConfig.zip".
3. Navigieren Sie zum Unterordner "pam". Dieser Ordner enthält die folgenden Dateien:

   pam-server.conf

   Wird für nicht sichere Konfigurationen verwendet.

   secure-pam-server.conf

   Wird für sichere Konfigurationen verwendet.

   pam-rest.conf

   Wird für REST-Konfigurationen verwendet.

   Bei diesen Dateien handelt es sich um spezifische Dateien für die Konfiguration von CA Process Automation mit NGINX.
4. Kopieren Sie diese drei Dateien, und fügen Sie sie in den folgenden Ordner ein:

   NGINX_Installationsverzeichnis/conf

   Sie können den NGINX-Lastenausgleich jetzt konfigurieren.

Grundlegende Kommunikation

Die folgenden Anweisungen beschreiben, wie grundlegende, nicht sichere Kommunikation für NGINX unter Windows- und Linux-Systemen konfiguriert wird.

Windows

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "pam-server.conf".

2. Öffnen Sie die Datei "pam-server.conf".

3. Es gibt drei Codeblocks, die für jeden Knoten, den Sie hinzufügen, bearbeitet werden müssen.

   a. Fügen Sie zum Block **upstream loadbalancer** den Hostnamen für node1 hinzu:
   `server <Enter node1 hostname here>:8080 max_fails=3 fail_timeout=3s`

   b. Fügen Sie zum Block **upstream jettyloadbalancer** den Hostnamen für node1 hinzu.
   `server <Enter node1 hostname here>:8080 max_fails=3 fail_timeout=3s`

   c. Fügen Sie zum Block **Define node1** den Hostnamen für node1 hinzu:
   `server <hostname of machine where you have installed node1>:<jetty server port> max_fails=3 fail_timeout=3s`

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

   Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

4. Speichern und schließen Sie die Datei "pam-server.conf".

5. Öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.

6. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:

   `include NGINX-Installationsverzeichnis/conf/pam-server.conf;`

   Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "pam-server.conf" für CA Process Automation vorgenommen haben.

7. Speichern und schließen Sie die Datei "nginx.conf".

   Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).

8. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.
9. Entfernen Sie Serverblocks aus dem Code, um Konflikte mit dem Server, der in der Datei "pam-server.conf" identifiziert wird, zu vermeiden.

   Zum Beispiel:

   ```
   server {
           listen       80;
           server_name  <LOADBALANCER_HOSTNAME>;
   location / {
                root   /usr/share/nginx/html;
                 index  index.html index.htm;
          }
   }
   ```

10. Speichern und schließen Sie die Datei "nginx.conf".
11. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis, und geben Sie Folgendes ein:

    ```
    nginx –s stop
    ```

12. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

Linux

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "nginx.conf".

2. Öffnen Sie die Datei "nginx.conf".

3. Geben Sie den Serverblock folgendermaßen an, um die eigenständige NGINX-Instanz zu verifizieren.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Speichern und schließen Sie die Datei.

5. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "pam-server.conf".

6. Öffnen Sie die Datei "pam-server.conf".

7. Es gibt drei Codeblocks, die für jeden Knoten, den Sie hinzufügen, bearbeitet werden müssen.

   a. Fügen Sie zum Block **upstream loadbalancer** den Hostnamen für node1 hinzu:
   `server <Enter node1 hostname here>:8080 max_fails=3 fail_timeout=3s`

   b. Fügen Sie zum Block **upstream jettyloadbalancer** den Hostnamen für node1 hinzu.
   `server <Enter node1 hostname here>:8080 max_fails=3 fail_timeout=3s`

   c. Fügen Sie zum Block **Define node1** den Hostnamen für node1 hinzu:
   `server <hostname of machine where you have installed node1>:<jetty server port> max_fails=3 fail_timeout=3s`

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

8. Speichern und schließen Sie die Datei "pam-server.conf".
9. Öffnen Sie die Datei "nginx.conf".
10. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:

    `include` *`NGINX-Installationsverzeichnis`*`/conf/pam-server.conf;`

    Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "pam-server.conf" für CA Process Automation vorgenommen haben.
11. Entfernen Sie den folgenden Eintrag:

    `include` *`NGINX_Installationsverzeichnis`*`/nginx/conf.d/*.conf;`
12. Speichern und schließen Sie die Datei "nginx.conf".

    Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).
13. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.
14. Entfernen Sie Serverblocks aus dem Code, um Konflikte mit dem Server, der in der Datei "pam-server.conf" identifiziert wird, zu vermeiden.

    Zum Beispiel:

    ```
    server {
            listen       80;
            server_name  <LOADBALANCER_HOSTNAME>;
    location / {
                 root   /usr/share/nginx/html;
                  index  index.html index.htm;
           }
    }
    ```
15. Speichern und schließen Sie die Datei "nginx.conf".
16. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis (nginx-1.42), und geben Sie Folgendes ein:

    `nginx –s stop`
17. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

Sichere Kommunikation

Die folgenden Anweisungen beschreiben, wie sichere Kommunikation für NGINX unter Windows- und Linux-Systemen konfiguriert wird. Im Gegensatz zur grundlegenden Kommunikation ist bei sicherer Kommunikation die Verwendung von Zertifikaten und Schlüsseldateien erforderlich.

Windows

Für die sichere Kommunikation für NGINX sind SSL-Zertifikate (die Dateien "c2okey2.pem" und "c2ocert.pem") erforderlich. Stellen Sie sicher, dass Sie diese Dateien generieren (siehe Seite 51), bevor Sie diesen Vorgang starten.

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner:

   NGINX_Installationsverzeichnis`/conf`

   Dieser Ordner enthält die Datei "secure-pam-server.conf".

2. Öffnen Sie die Datei "secure-pam-server.conf".

3. Es gibt drei Codeblocks, die für jeden Knoten, den Sie hinzufügen, bearbeitet werden müssen. Bearbeiten Sie die Blocks entsprechend Ihren Sicherheitsvorkehrungen.

   a. Fügen Sie zum Block **upstream loadbalancer** den Hostnamen für node1 hinzu:
   `server <Enter node1 hostname here>:8443 max_fails=3 fail_timeout=3s`

   b. Fügen Sie zum Block **upstream jettyloadbalancer** den Hostnamen für node1 hinzu.
   `server <Enter node1 hostname here>:8443 max_fails=3 fail_timeout=3s`

   c. Fügen Sie zum Block **Define node1** den Hostnamen für node1 hinzu:
   `server <hostname of machine where you have installed node1>:<jetty server port> max_fails=3 fail_timeout=3s`

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

   Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

4. Aktualisieren Sie die folgenden Zeilen, indem Sie den Speicherort der Dateien "c2ocert.pem" und "c2okey2.pem" angeben (im Verzeichnis "NGINX_Installationsverzeichnis\conf directory").

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   Zum Beispiel:

   ```
   ssl_certificate
   <NGINX_Installationsverzeichnis\conf\c2ocert.pem>;
   ```

5. Speichern und schließen Sie die Datei "secure-pam-server.conf".
6. Öffnen Sie die Datei "nginx.conf".
7. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:
   `include` *`NGINX-Installationsverzeichnis`*`/conf/secure-pam-server.conf;`

   Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "secure-pam-server.conf" für CA Process Automation vorgenommen haben.
8. Speichern und schließen Sie die Datei "nginx.conf".

   Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).
9. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.
10. Entfernen Sie Serverblocks aus dem Code, um Konflikte mit dem Server, der in der Datei "secure-pam-server" identifiziert wird, zu vermeiden.

    Zum Beispiel:

    ```
    server {
            listen       80;
            server_name  <LOADBALANCER_HOSTNAME>;
    location / {
                 root   /usr/share/nginx/html;
                  index  index.html index.htm;
           }
    }
    ```

11. Speichern und schließen Sie die Datei "nginx.conf".
12. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis (nginx-1.42), und geben Sie Folgendes ein:

    ```
    nginx –s stop
    ```

13. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

Linux

Für die sichere Kommunikation für NGINX sind SSL-Zertifikate (die Dateien "c2okey2.pem" und "c2ocert.pem") erforderlich. Stellen Sie sicher, dass Sie diese Dateien generieren (siehe Seite 51), bevor Sie diesen Vorgang starten.

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "nginx.conf".

2. Öffnen Sie die Datei "nginx.conf".

3. Geben Sie den Serverblock folgendermaßen an, um die eigenständige NGINX-Instanz zu verifizieren.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Speichern und schließen Sie die Datei.

5. Wechseln Sie zum folgenden Ordner:

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "secure-pam-server.conf".

6. Öffnen Sie die Datei "secure-pam-server.conf".

7. Es gibt drei Codeblocks, die für jeden Knoten, den Sie hinzufügen, bearbeitet werden müssen. Bearbeiten Sie die Blocks entsprechend Ihren Sicherheitsvorkehrungen.

   a. Fügen Sie zum Block **upstream loadbalancer** den Hostnamen für node1 hinzu:
   `server <Enter node1 hostname here>:8443 max_fails=3 fail_timeout=3s`

   b. Fügen Sie zum Block **upstream jettyloadbalancer** den Hostnamen für node1 hinzu.
   `server <Enter node1 hostname here>:8443 max_fails=3 fail_timeout=3s`

   c. Fügen Sie zum Block **Define node1** den Hostnamen für node1 hinzu:
   `server <hostname of machine where you have installed node1>:<jetty server port> max_fails=3 fail_timeout=3s`

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

   Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

8. Aktualisieren Sie die folgenden Zeilen, indem Sie den Speicherort der Dateien "c2ocert.pem" und "c2okey2.pem" angeben (im Verzeichnis "NGINX_Installationsverzeichnis\conf directory").

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   Zum Beispiel:

   ```
   ssl_certificate
   <NGINX_Installationsverzeichnis\conf\c2ocert.pem>;
   ```

9. Speichern und schließen Sie die Datei "secure-pam-server.conf".
10. Öffnen Sie die Datei "nginx.conf".
11. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:

    `include NGINX-Installationsverzeichnis/conf/pam-server.conf;`

    Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "secure-pam-server.conf" für CA Process Automation vorgenommen haben.
12. Entfernen Sie den folgenden Eintrag aus:

    `include NGINX_Installationsverzeichnis/nginx/conf.d/*.conf;`
13. Speichern und schließen Sie die Datei "nginx.conf".

    Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).
14. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.
15. Entfernen Sie Serverblocks aus dem Code, um Konflikte mit dem Server, der in der Datei "secure-pam-server.conf" identifiziert wird, zu vermeiden.

    Zum Beispiel:

    ```
    server {
            listen       80;
            server_name  <LOADBALANCER_HOSTNAME>;
    location / {
                root   /usr/share/nginx/html;
                 index  index.html index.htm;
           }
    }
    ```
16. Speichern und schließen Sie die Datei "nginx.conf".
17. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis (nginx-1.42), und geben Sie Folgendes ein:

    `nginx –s stop`
18. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

REST-Konfiguration

Es besteht die Möglichkeit, in CA Process Automation einen NGINX-Lastenausgleich für die Catalyst-RESTful-API zu konfigurieren. In den folgenden Anweisungen wird beschrieben, wie sie Ihren NGINX-Lastenausgleich konfigurieren sollten, um REST für grundlegende und sichere Kommunikation sowohl auf Windows- als auch auf Linux-Systemen zu verwenden.

Grundlegende Kommunikation

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "pam-rest.conf".

2. Öffnen Sie die Datei "pam-rest.conf".

3. Bearbeiten Sie den folgenden Codeblock:

   ```
   HTTP
   upstream ucfcluster  {
     server <Enter node1 hostname here>:7000 max_fails=3
   fail_timeout=5s;
     server <Enter node2 hostname here>:7000 max_fails=3
   fail_timeout=5s;
   }
   ```

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

   Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

4. Speichern und schließen Sie die Datei "pam-rest.conf".

5. Öffnen Sie die Datei "nginx.conf".

6. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:
   `include NGINX-Installationsverzeichnis/conf/pam-rest.conf;`

   Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "pam-rest.conf" für CA Process Automation vorgenommen haben.

7. Speichern und schließen Sie die Datei "nginx.conf".

   Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).

8. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.

9. Speichern und schließen Sie die Datei "nginx.conf".

10. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis (nginx-1.42), und geben Sie Folgendes ein:

    ```
    nginx –s stop
    ```

11. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

Sichere Kommunikation

Für sichere Kommunikation mit REST sind SSL-Zertifikatsdateien erforderlich. Stellen Sie sicher, dass Sie diese Dateien generieren (siehe Seite 51), bevor Sie diesen Vorgang starten.

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner

   NGINX_Installationsverzeichnis/conf

   Dieser Ordner enthält die Datei "pam-rest.conf".

2. Öffnen Sie die Datei "pam-rest.conf".

3. Bearbeiten Sie den folgenden Codeblock:

   ```
   ## HTTPS
   upstream sslcluster  {
     server <Enter node1 hostname here>:7443 max_fails=3
   fail_timeout=5s;
     server <Enter node2 hostname here>:7443 max_fails=3
   fail_timeout=5s;
   }
   ```

   Ersetzen Sie den Platzhalter *Enter node1 hostname here* jeweils durch einen gültigen Wert. Ändern Sie die Portnummern nicht, außer, Sie verwenden für den CA Process Automation-Knoten einen abweichenden Port.

   Wiederholen Sie diese Schritte für alle zusätzlichen Knoten, die Sie installieren.

4. Aktualisieren Sie die folgenden Zeilen, indem Sie den Speicherort der Dateien "c2ocert.pem" und "c2okey2.pem" angeben (im Verzeichnis "NGINX_Installationsverzeichnis\conf directory").

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   Zum Beispiel:

   ```
   ssl_certificate
   <NGINX_Installationsverzeichnis\conf\c2ocert.pem>;
   ```

5. Speichern und schließen Sie die Datei "pam-rest.conf".

6. Öffnen Sie die Datei "nginx.conf".

7. Fügen Sie am Ende der nginx.conf-Datei die folgende Eingabe im http-Block hinzu:
   `include NGINX-Installationsverzeichnis/conf/pam-rest.conf;`

   Diese Eingabe verknüpft NGINX mit den Konfigurationsänderungen, die Sie in der Datei "pam-rest.conf" für CA Process Automation vorgenommen haben.

8. Speichern und schließen Sie die Datei "nginx.conf".

   Wichtig! Führen Sie die restlichen Schritte aus, *nachdem* Sie mindestens einen Koordinationsrechner-Knoten installiert haben. Anweisungen finden Sie unter Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95) oder Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121).

9. Wenn Sie mindestens einen Koordinationsrechner-Knoten installiert haben, öffnen Sie die Datei *NGINX-Installationsverzeichnis*/conf/nginx.conf.

10. Speichern und schließen Sie die Datei "nginx.conf".

11. Stoppen Sie NGINX. Navigieren Sie in einer Eingabeaufforderung zum NGINX-Verzeichnis (nginx-1.42), und geben Sie Folgendes ein:

    `nginx –s stop`

12. Starten Sie NGINX neu.

    Die Änderungen werden nun wirksam.

Generieren von SSL-Zertifikatsdateien

Die SSL-Zertifikate müssen *nach* der Installation von CA Process Automation und *vor* der Konfiguration von sicherer Kommunikation für Ihren Lastenausgleich generiert werden. SSL-Zertifikate sind nicht erforderlich, wenn Sie für Ihren Lastenausgleich grundlegende, nicht sichere Kommunikation verwenden möchten.

Nachdem das Zertifikat generiert wurde, muss der Speicherort der Zertifikatsdatei identifiziert werden, wenn Sie Ihren Lastenausgleich für sichere Kommunikation konfigurieren.

Gehen Sie folgendermaßen vor:

1. Laden Sie OpenSSL von einem Drittanbieter herunter, und installieren Sie es.

   Hinweis: Stellen Sie sicher, dass auf dem Host, auf dem Sie OpenSSL installieren, JDK installiert ist.

2. Nachdem Sie CA Process Automation im Clustermodus installiert haben (und mindestens ein Knoten installiert wurde), generiert der CA Process Automation-Installationsassistent die Datei "c2okeystore" am folgenden Speicherort:

   `\server_location\c2o\.config`

   Kopieren Sie die Datei "c2okeystore", und fügen Sie sie im folgenden Verzeichnis ein:

   `\jdk_location\bin`

   Sie können die Befehle lokal von diesem Speicherort aus ausführen.

3. Verwenden Sie "keytool" in JDK, um den Schlüsselspeicher wie folgt in das pksc12-Format zu importieren:

   a. Gehen Sie zum Verzeichnis "jdk_location\bin", und führen Sie den folgenden Befehl aus:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      Sie werden in der Konsole aufgefordert, das Kennwort des Zielschlüsselspeichers einzugeben.

      Hinweis: Das Schlüsselspeicherkennwort befindet sich in der Datei "OasisConfig.properties". Suchen Sie die Datei im folgenden Verzeichnis: `\server_location\c2o\.config\`

      Öffnen Sie die Datei, und kopieren Sie das Kennwort. Der Wert befindet sich neben der Eingabe "KEYSTOREID=".

      Beispiel: KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. Das Kennwort ist 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Fügen Sie das Kennwort in die Aufforderung zur Eingabe des Zielschlüsselspeicher-Kennworts in Ihrer offenen Konsole ein.

   c. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort wiederholt ein.

   d. Geben Sie das Kennwort in der Aufforderung zur Eingabe des Quellschlüsselspeicher-Kennworts erneut ein.

      Im Verzeichnis \jdk_location\bin wird eine Datei namens "c2okeystore.p12" generiert.

   e. Sie müssen den Schlüsselspeicher im p12-Format in Schlüssel- und Zertifikatsdateien im PEM-Format konvertieren. Führen Sie dazu im Verzeichnis \jdk_location\bin den Befehl "openssl" aus:

```
openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
```

f. Geben Sie das Schlüsselspeicherkennwort in der Aufforderung zur Eingabe des Kennworts ein.

g. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase eine beliebige Phrase ein.

h. Geben Sie Ihre PEM-Passphrase erneut ein.

i. Führen Sie den folgenden Befehl im Verzeichnis \jdk_location\bin aus:
```
openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem
```

j. Geben Sie das Schlüsselspeicherkennwort in der Aufforderung zur Eingabe des Kennworts ein.

k. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase dieselbe Phrase ein, die in Schritt g erstellt haben.

l. Geben Sie Ihre PEM-Passphrase erneut ein.

m. Führen Sie den folgenden Befehl im Verzeichnis \jdk_location\bin aus:
```
openssl rsa -in c2okey.pem -out c2okey2.pem
```

n. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase dieselbe Phrase ein, die in Schritt g erstellt haben.

o. Geben Sie Ihre PEM-Passphrase erneut ein.

p. Kopieren Sie die Dateien "c2okey2.pem" und "c2ocert.pem" in das Verzeichnis \conf Ihres Lastenausgleichs.

Hinweis: Erstellen Sie Sicherheitskopien dieser Dateien.

Voraussetzungen des F5-Lastenausgleichs

Jeder geclusterte Koordinationsrechner benötigt einen Lastenausgleich. Wenn Sie einen F5-Lastenausgleich verwenden, können Sie diesen verwenden, um Operator- oder Webservice-Anfragen auf geclusterten Knoten des Ziel-Koordinationsrechners zu verteilen.

Bevor Sie den ersten Knoten von einem geclusterten Domänen-Koordinationsrechner oder einem anderen geclusterten Koordinationsrechner installieren, bereiten Sie F5 zur Ausführung des Lastenausgleichs vor.

Sammeln Sie zuerst folgende Informationen:

- Identität von Servern oder virtuellen Servern, auf denen Koordinationsrechner-Knoten bereitgestellt werden sollen.
- Anmeldeinformationen, um sich bei der F5-Schnittstelle anzumelden.

Sie müssen folgende F5-Elemente so konfigurieren, dass sie mit CA Process Automation funktionieren.

1. Erstellen eines F5-Knoten für jeden Cluster-Knoten (siehe Seite 55).

   Für CA Process Automation ist ein Knoten ein beliebiger Host oder virtueller Server, auf dem ein Cluster-Knoten des Koordinationsrechners installiert ist (oder in der Zukunft installiert werden könnte).

2. Erstellen eines F5-Pools für jeden CA Process Automation-Cluster (siehe Seite 56).

   Für CA Process Automation schließt jeder Pool die Cluster-Knoten des Koordinationsrechners ein, die zum gleichen geclusterten Koordinationsrechner gehören.

3. Erstellen einer F5 iRule für CA Process Automation (siehe Seite 57).

   Für CA Process Automation leitet iRule Operatoranfragen weiter, die auf den Kontaktpunkt eines geclusterten Koordinationsrechners abzielen.

4. Erstellen Sie einen virtuellen Server von F5 für CA Process Automation (siehe Seite 60).

   F5 kann einige virtuelle Server aufweisen. CA Process Automation wird als einer der virtuellen Server eingerichtet.

5. Konfigurieren Sie F5, um vereinfachte Kommunikation mit HTTPS zu verwenden (siehe Seite 62).

6. Bereiten Sie den F5-Lastenausgleich für die Kommunikationsüberprüfung vor (siehe Seite 64).

7. Aktivieren Sie allgemeingültige Sitzungen im F5-Lastenausgleich. Allgemeingültige Sitzungen müssen auf F5 aktiviert werden, damit sie mit einem CA Process Automation-Cluster funktionieren.

Erstellen eines F5-Knoten für jeden Cluster-Knoten

Anstatt die Cluster-Knoten zu konfigurieren, nachdem sie in CA Process Automation vorhanden sind, konfigurieren Sie die Knoten, die Sie einem geclusterten Koordinationsrechner im Vorfeld hinzufügen möchten.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei F5 an.
2. Wählen Sie die Registerkarte "Main" aus, klicken Sie auf "Local Traffic", und klicken Sie anschließend auf "Nodes".

   Die Knotenliste zeigt folgende Details für jeden Netzwerkknoten an, der für F5 definiert wurde: Der Status, die IP-Adresse, die Partition und der Hostname.
3. Klicken Sie auf "Erstellen".

   Die Seite "New Node" wird angezeigt.
4. Füllen Sie den Abschnitt "General Properties" aus.

   Adresse

   Gibt die IP-Adresse des neuen Knotens an.

   Name

   Gibt den Hostnamen der zugeordneten IP-Adresse an.
5. Füllen Sie den Konfigurationsabschnitt aus.

   Health Monitors

   Gibt den Zustandsmonitor für diesen Knoten an. Wenn er nicht konfiguriert ist, wählen Sie "Keine" aus.

   Standard: Node Default

   Ratio

   Gibt einen gewichteten Wert an, der einem Knoten zugewiesen wird. Wenn die Knoten, die dem gleichen Cluster angehören, alle über die gleiche Kapazität verfügen, geben Sie für jeden Knoten den Wert 1 für "Ratio" ein.

   Connection Limit

   Gibt die Höchstanzahl von Verbindungen an, die dieser Knoten verarbeiten kann.
6. Klicken Sie auf "Fertig".

   Der hinzugefügte Knoten wird in der Knotenliste angezeigt.

Erstellen von zwei F5-Pools für jeden CA Process Automation-Cluster

Erstellen Sie zwei F5-Pools für jeden CA Process Automation-Cluster. Fügen Sie jedem F5-Pool, den Sie erstellen, die Knoten hinzu, die dem zugeordneten Cluster angehören.

Erstellen Sie beispielsweise zwei Pools wie in folgenden Beispielen:

- PAMPOOL namens PAMSRVPOOL, wobei Mitglieder Port 8080 (grundlegend) oder Port 8443 (sicher) verwenden. Dieser Pool wird für alle Kommunikationsvorgänge verwendet.
- PAMWSPOOL PAMJETTYPOOL, wobei Mitglieder Port 80 (grundlegend) oder Port 443 (sicher) verwenden. Dieser Pool unterstützt Agenten, die für vereinfachte Kommunikation mit Web-Sockets konfiguriert sind.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei F5 an.
2. Wählen Sie die Registerkarte "Main" aus, klicken Sie auf "Local Traffic", und klicken Sie anschließend auf "Pools".

   Die Pool-Liste ist leer, wenn Sie das erste Mal Pools einrichten. Die Pool-Liste zeigt folgende Details für jeden Pool an: Status, Pool-Name, Partition und Anzahl der Mitglieder im Pool.
3. Klicken Sie auf "Erstellen".

   Die Seite "New Pool" wird angezeigt.
4. Füllen Sie den Konfigurationsabschnitt aus.
   a. Wählen Sie "Basic" in der Drop-down-Liste aus.
   b. Geben Sie einen Namen für den neuen Pool ein.
   c. Wählen Sie von den verfügbaren Zustandsmonitoren "http" aus, und verschieben Sie es in die aktive Liste.
5. Wählen Sie "Round Robin" aus der Drop-down-Liste "Load Balancing Method" aus.
6. Wählen Sie "Disabled" aus der Drop-down-Liste "Priority Group Activation" aus.
7. Fügen Sie dem neuen F5-Pool jeden Knoten folgendermaßen hinzu:
   a. Wählen Sie "Knotenliste" aus, da Sie einen definierten Knoten hinzufügen.
   b. Wählen Sie die "IP-Address" (Hostname) aus der Drop-down-Liste "Address" aus, die den Knoten identifiziert, der diesem F5-Pool hinzugefügt werden soll.
   c. Geben Sie für den Serviceport basierend auf Sicherheitsebene (grundlegend oder sicher) und Typ (veraltet oder vereinfacht) der Kommunikation einen der folgenden Werte an:

      Grundlegende (nicht sichere) und veraltete Kommunikation

      8080

      Grundlegende (nicht sichere) und vereinfachte Kommunikation

80 (Wählen Sie "HTTP" aus. Das Feld "Service Port" wird automatisch mit 80 aufgefüllt.)

Sichere und veraltete Kommunikation

8443

Sichere und vereinfachte Kommunikation

443 (Wählen Sie "HTTPS" aus. Das Serviceport-Feld wird automatisch mit 443 aufgefüllt.)

d. Klicken Sie auf Hinzufügen.

Die Details, die Sie für diesen Knoten hinzugefügt haben, werden in der Liste "New Members" angezeigt.

8. Klicken Sie auf "Fertig".

Der neue Pool wird der F5-Pool-Liste hinzugefügt.

Erstellen einer F5 iRule für CA Process Automation

Eine iRule leitet Operatoranfragen weiter, die auf den Kontaktpunkt eines geclusterten Koordinationsrechners abzielen. F5 erstellt eine URL aus diesen Informationen und verwendet diese URL als Kontaktpunktziel. Um eine F5 iRule für CA Process Automation zu erstellen, kopieren Sie die angegebene iRule-Definition in das Textfeld "Beschreibung". Legen Sie dann die Werte für die Variable "*MyPool*" fest.

Hinweis: Eine iRule entspricht "uriworkermap.properties" in Apache. Eine iRule identifiziert einen Cluster-Knoten des Koordinationsrechners für eine Anfrage, die auf den Kontaktpunkt eines geclusterten Koordinationsrechners abzielt. Die Entscheidung basiert auf der URL.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei F5 an.
2. Wählen Sie die Registerkarte "Main" aus, klicken Sie auf "Local Traffic", und klicken Sie anschließend auf "iRules".

   Die iRules-Liste ist leer, wenn Sie das erste Mal iRules einrichten. Die iRules-Liste zeigt folgende Details für jedes iRule an: Den iRule-Namen und die Partition.
3. Klicken Sie auf "Erstellen".

   Die Seite "New iRule" wird angezeigt.

4. Füllen Sie den Abschnitt "Properties" aus.

   Name

   Gibt den iRule-Namen an.

   Definition

   Gibt die iRule-Definition an. Kopieren Sie den Text aus The iRule Definition (siehe Seite 59) in dieses Textfeld.

   Hinweis: Die für iRules verwendete Programmiersprache ist "Tcl" (Tool Command Language).

   Extend Text Area

   Gibt an, ob der Textbereich im Textfeld "Definition" auf die maximale Größe erweitert werden soll.

   Aktiviert: Der Textbereich wird auf die maximale Größe erweitert.

   Deaktiviert: Der Textbereich wird in einer Größe dargestellt, die kleiner als die maximale Größe ist.

   Wrap Text

   Gibt an, ob der Text mit einem Zeilenumbruch formatiert wird, um sich an das Textfeld "Definition" anzupassen, statt eine horizontale Bildlaufleiste anzuzeigen.

   Aktiviert: Der Text, der über den sichtbaren Teil des Textfeldes "Definition" hinausgeht, ausgenommen der horizontalen Bildlaufleiste, wird mit einem Zeilenumbruch formatiert.

   Deaktiviert: Der Text wird wie eingegeben angezeigt, bei Bedarf mit einer horizontalen Bildlaufleiste.

5. Klicken Sie auf "Fertig".

   Die von Ihnen eingegebene iRule wird in der iRule-Liste angezeigt.

Die iRule-Definition

Geben Sie für Ihre neue iRule folgende Definition in das Textfeld "Definition" ein. Passen Sie die Werte für die festgelegten Anweisungen an Ihre spezifischen Anforderungen an.

- Verwenden Sie für die Variable "BasicPool" spezifische Werte für den aktuellen Pool mit Port 8080 für grundlegende (nicht sichere) Kommunikation.
- Legen Sie für die IP-Adressen für NODE1 und NODE2 Werte der Server im PAMWSPOOL-Pool fest.
- Verwenden Sie "set WSPORT "80"" für HTTP oder "set WSPORT "443"" für HTTPS, um den Port für vereinfachte Kommunikation festzulegen.

```
when HTTP_REQUEST {
set PAMPOOL "PAMSRVRPOOL"
set PAMWSPOOL "PAMJETTYPOOL"
set NODE1 "10.130.5.146"
set NODE2 "10.130.5.147"
set WSPORT "80"
    switch -glob [HTTP::uri] {
        "/jmx-console*" { pool $PAMPOOL }
        "/web-console*" { pool $PAMPOOL }
        "/c2orepository/*" { pool $PAMPOOL }
        "/c2orepository/oasisHelp*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/aboutUs/*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/language/*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/installation/*" { pool $PAMPOOL }
        "/c2orepository/media*" { pool $PAMPOOL }
        "/c2orepository/thirdParty*" { pool $PAMPOOL }
        "/c2orepository/MainInstallerConfiguration.properties" {
        pool $PAMPOOL }
        "/itpam*" { pool $PAMPOOL }
        "/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL }
        "/itpam/MirroringRequestProcessor*" { pool $PAMPOOL }
        "/itpam/AgentConfigurationRequestServlet" { pool $PAMPOOL }
        "/itpam/StartAgent*" { pool $PAMPOOL }
        "/itpam/OasisPrimary" { pool $PAMPOOL }
        "/itpam/JNLPRequestProcessor*" { pool $PAMPOOL }
        "/itpam/JNLPRequestProcessor/installation" { pool $PAMPOOL }
        "/itpam/clientproxy/c2oresourceaction" { pool $PAMPOOL }
        "/itpam/clientproxy/c2oreportaction" { pool $PAMPOOL }
        "/mirroringrepository*" { pool $PAMPOOL }
        "/birt/*" { pool $PAMPOOL }
        default { pool $PAMPOOL }
        "/ws/node1" { pool $PAMWSPOOL member $NODE1 $WSPORT }
          "/ws/node1/*" { pool $PAMWSPOOL member $NODE1 $WSPORT }
        "/ws/node2" { pool $PAMWSPOOL member $NODE2 $WSPORT }
          "/ws/node2/*" { pool $PAMWSPOOL member $NODE2 $WSPORT }
        "/*" { pool $PAMWSPOOL }
    }
```

```
}
```

Erstellen eines virtuellen Servers von F5 für CA Process Automation

Sie können einen virtuellen Server von F5 erstellen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei F5 an.
2. Wählen Sie die Registerkarte "Main" aus, klicken Sie auf "Local Traffic", und klicken Sie anschließend auf "Virtual Servers".

   Die "Virtual Servers List" zeigt folgende Details für jeden virtuellen Server an: Status, Name, Partition, Ziel-IP-Adresse, Serviceport, Typ und eine Verknüpfung zum Bearbeiten von Ressourcen.
3. Klicken Sie auf "Erstellen".

   Die Seite "New Virtual Server" wird angezeigt.
4. Füllen Sie den Abschnitt "General Properties" aus.

   Name

   Gibt den Namen des virtuellen Servers an, zum Beispiel "PAMLB".

   Destination Type

   Gibt den Host für eine einzelne IP-Adresse an.

   Destination Address

   Gibt die IP-Adresse des virtuellen Servers an, zum Beispiel "10.130.5.149".

   Service Port

   Gibt den zugeordneten Port für den virtuellen Server an, zum Beispiel 80 für HTTP, 443 an HTTPS.

   Zustand

   Gibt an, ob der virtuelle Server für Lastenausgleich verfügbar ist. Geben Sie "Enabled" an.

5. Füllen Sie den Konfigurationsabschnitt aus. Akzeptieren Sie alle Standards, außer "HTTP Profile".

   Typ

   Gibt den Typ des virtuellen Servers an. "Standard" ist ein virtueller Server, der den gesamten Datenverkehr an den Pool richtet, den Sie als standardmäßigen Pool für Lastenausgleich definiert haben.

   Standard: Standard

   HTTP Profile

   Gibt das HTTP-Profil zur Verwaltung des HTTP-Datenverkehrs an. Wählen Sie "http" aus.

6. Füllen Sie den Abschnitt "Resources" aus.

   iRules

   Gibt die iRules an, die für diesen virtuellen Server aktiviert werden sollen. Wählen Sie das iRules-Skript aus, das Sie für den geclusterten Koordinationsrechner erstellt haben.

   Schließen Sie die iRule ein, die Sie für den Standardpool erstellt haben.

   Default Pool

   Gibt den Namen des Pools an, zu dem der virtuelle Server den Datenverkehr weiterleitet. Geben Sie den CA Process Automation-Pool als Standardpool an.

   Default Persistence Profile

   Gibt das Persistenzprofil für diesen virtuellen Server an. Zum Beispiel "source_addr".

   Fallback Persistence Profile

   Gibt das Persistenzprofil an, das dieser virtuelle Server verwendet, wenn das standardmäßige Persistenzprofil nicht verwendet werden kann. Zum Beispiel "dest_addr".

7. Klicken Sie auf "Fertig".

Konfigurieren von F5 für die Verwendung von vereinfachter Kommunikation mit HTTPS

Für SSL-Kommunikation in F5 sind eine Zertifikatsdatei und eine Schlüsseldatei erforderlich. Für vereinfachte Kommunikation können nur Zertifikate verwendet werden, die durch keytool generiert und in den CA Process Automation-Schlüsselspeicher kopiert wurden.

Gehen Sie folgendermaßen vor:

1. Generieren Sie SSL-Zertifikatsdateien (siehe Seite 51).
2. Laden Sie das SSL-Zertifikat und den Schlüssel hoch.
   a. Melden Sie sich bei F5 an.
   b. Klicken Sie auf "Local Traffic", "SSL Certificates", "Import".
   c. Importieren Sie den Schlüssel: Wählen Sie als Importtyp "Key" aus, geben Sie den Schlüsselnamen ein, klicken Sie auf "Browse", navigieren Sie zum Speicherort der Schlüsseldatei, und klicken Sie auf "Import".

      Anwenderspezifischer_Speicherort/c2okey2.pem
   d. Klicken Sie auf "Local Traffic", "SSL Certificates", "Import".
   e. Importieren Sie das Zertifikat: Wählen Sie als Importtyp "Certificate" aus, geben Sie den Zertifikatsnamen ein, klicken Sie auf "Browse", navigieren Sie zum Speicherort des Zertifikats, und klicken Sie auf "Import".

      Anwenderspezifischer_Speicherort/c2ocert2.pem
3. Erstellen Sie das Client-Profil.
   a. Klicken Sie auf "Local Traffic", "Profiles", "SSL", "Client".
   b. Klicken Sie auf "Erstellen".
   c. Geben Sie im Feld "Name" einen Namen ein. Akzeptieren Sie für "Parent Profile" den Standardwert "clientssl".
   d. Wählen Sie unter "Configuration" "Advanced" aus.
   e. Aktivieren Sie im rechten Bereich die Felder "Certificate", "Key" und "Pass Phrase", um sie editierbar zu machen.
   f. Wählen Sie in der Drop-down-Liste "Certificate" das Zertifikat "c2ocert2.pem" aus, das Sie im vorigen Schritt importiert haben.
   g. Wählen Sie in der Drop-down-Liste "Key" den Schlüssel " c2okey2.pem" aus, den Sie im vorigen Schritt importiert haben.
   h. Geben Sie in den Feldern "Pass Phrase" und "Confirm Pass Phrase" die Schlüsselwortfolge ein, die für das Generieren der Zertifikatsdateien verwendet wurde.
   i. Klicken Sie auf "Fertig".

4. Erstellen Sie das Serverprofil.
   a. Klicken Sie auf "Local Traffic", "Profiles", "SSL", "Server".
   b. Klicken Sie auf "Erstellen".
   c. Geben Sie im Feld "Name" einen Namen ein. Akzeptieren Sie für "Parent Profile" den Standardwert "serverssl".
   d. Wählen Sie unter "Configuration" "Advanced" aus.
   e. Aktivieren Sie im rechten Bereich die Felder "Certificate", "Key" und "Pass Phrase", um sie editierbar zu machen.
   f. Wählen Sie in der Drop-down-Liste "Certificate" das Zertifikat "c2ocert2.pem" aus, das Sie im vorigen Schritt importiert haben.
   g. Wählen Sie in der Drop-down-Liste "Key" den Schlüssel " c2okey2.pem" aus, den Sie im vorigen Schritt importiert haben.
   h. Geben Sie in den Feldern "Pass Phrase" und "Confirm Pass Phrase" die Schlüsselwortfolge ein, die für das Generieren der Zertifikatsdateien verwendet wurde.
   i. Klicken Sie auf "Fertig".
5. Verknüpfen Sie die Client- und Serverprofile mit dem virtuellen F5-Server.
   a. Klicken Sie auf "Local Traffic", "Virtual Servers", "Virtual Server List".
   b. Wählen Sie den virtuellen Server für CA Process Automation, beispielsweise "pamlib", aus.

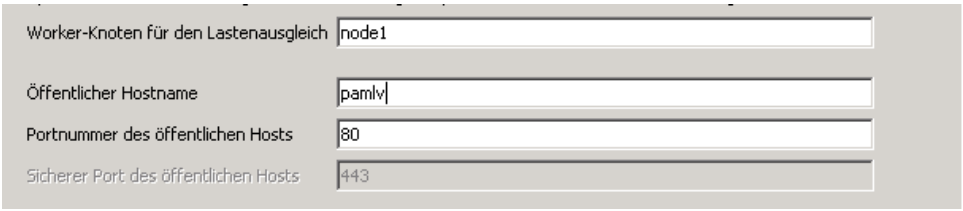
      Beachten Sie, dass für den Service-Port 443 sowie HTTPS angezeigt wird.
   c. Wählen Sie für "SSL Profile" (Client) "clientssl" aus (der Standardwert, den Sie in den zwei vorhergehenden Schritten als übergeordnetes Profil verwendet haben).
   d. Wählen Sie für "SSL Profile" (Server) "serverssl" aus.
   e. Klicken Sie auf "Fertig".

Vergleich der Porteinstellungen für HTTPS und HTTP

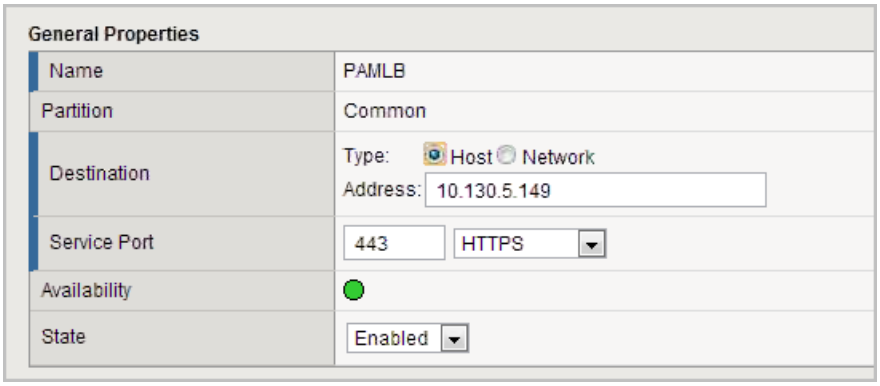
	HTTPS (sicher)	HTTP (grundlegend)
Service Port	443	80
Zum Pool hinzugefügte Knotenmitglieder	8443	8080
Auf Web-Socket-Port verweisende iRule	443	80

Vorbereiten des F5-Lastenausgleichs für die Kommunikationsüberprüfung (Beispiel)

Der Installationsprozess des Koordinationsrechners präsentiert eine Konfigurationsseite, wo Sie die Konfiguration eines Lastenausgleichs auswählen können:



In der CA Process Automation-Installation geben Sie für "Öffentlicher Hostname" den Hostnamen ein, den Sie in F5 angeben. Um zu validieren, dass CA Process Automation mit dem in "Öffentlicher Hostname" angegebenen Host kommunizieren kann, sendet der CA Process Automation-Installationsprozess eine HTTP GET-Anfrage an das von Ihnen angegebene Ziel. Das Problem für den CA Process Automation-Installationsprozess ist, dass dieser Hostname zu einer privaten IP-Adresse des virtuellen Servers zugeordnet ist, den F5 zuweist -- eine IP-Adresse, die kein Teil Ihres lokalen CA Process Automation-Netzwerks ist. Im folgenden Beispiel ist "10.130.5.149" eine IP-Adresse, die Teil des F5-Netzwerks ist, und nicht des CA Process Automation-Netzwerks.



Ohne Umgehungslösung tritt ein Fehler auf, der folgendem Fehler ähnelt:

```
java.net.UnknownHostException:pamlb
```

Um die Kommunikationsvalidierung erfolgreich abzuschließen, erstellen Sie eine Eingabe in Ihrer Hosts-Datei, die Ihre Eingabe für "Öffentlicher Hostname" zu einer IP-Adresse eines Servers zuordnet, der auf diese Anfrage reagieren kann.

Erstellen Sie zum Beispiel eine Eingabe zur Hosts-Datei, die Ihre Eingabe für "Öffentlicher Hostname" zu einer IP-Adresse eines Servers im CA Process Automation-Netzwerk, in dem ein Apache-Lastenausgleich installiert ist, zuordnet.

```
xxx.xxx.xxx.xxx      pamlb
```

Nachdem das Installationsprogramm nach der Lastenausgleichsseite fortgefahren ist, entfernen Sie diese Umgehungszeile aus der Hosts-Datei.

Hinweis: Alternativ können Sie F5 konfigurieren, sodass die zugewiesene IP-Adresse die "open http stream"-Anfrage vom Installationsprozess des CA Process Automation-Koordinationsrechners akzeptieren kann. Weitere Informationen hierzu finden Sie in der F5-Dokumentation.

Weitere Informationen:

Vom Lastenausgleich verwendete Ports (siehe Seite 235)

Kapitel 5: Installieren des Domänen-Koordinationsrechners

Der Domänen-Koordinationsrechner wird installiert, wenn Sie CA Process Automation das erste Mal installieren. Bevor Sie den Domänen-Koordinationsrechner installieren, müssen Sie die Voraussetzungen erfüllen. Sie können den Domänen-Koordinationsrechner über einen Assistenten interaktiv installieren. Oder Sie können eine Antwortdatei mit Werten für Parameter erstellen, die keine Standards haben und dann das Skript ausführen, um den Domänen-Koordinationsrechner automatisch zu installieren. Konfigurieren Sie Ports und Firewalls nach der Installation. Konfigurieren Sie anschließend CA Process Automation, wie im *Handbuch für Inhaltsadministratoren* beschrieben.

Dieses Kapitel enthält folgende Themen:

Voraussetzungen zur Installation des Domänen-Koordinationsrechners (siehe Seite 67)
Interaktive Installation des Domänen-Koordinationsrechners (siehe Seite 95)
Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121)
Aufgaben nach der Installation für den Domänen-Koordinationsrechner (siehe Seite 128)
Deinstallieren des Domänen-Koordinationsrechners (siehe Seite 144)

Voraussetzungen zur Installation des Domänen-Koordinationsrechners

Erwägen Sie, für Ihre erste Installation einen Lastenausgleich zu implementieren, um auf spätere Erweiterungen vorbereitet zu sein. (Bei Bedarf können Cluster-Knoten hinzugefügt werden.)

Hinweis: Es wird empfohlen, einen hardwarebasierten Lastenausgleich zu verwenden. Weitere Informationen finden Sie unter Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54). Wenn dies nicht möglich ist, wird NGINX als bevorzugter softwarebasierter Lastenausgleich empfohlen. NGINX für UNIX ist hochgradig skalierbar. NGINX für Windows kann bis zu 300 Agenten, die vereinfachte Kommunikation verwenden, unterstützen. Weitere Informationen finden Sie unter Voraussetzungen des NGINX-Lastenausgleichs.

Planen Sie Ihre Erstinstallation von CA Process Automation. Informationen zu Komponentenanforderungen finden Sie unter:

- Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
- Hardwareanforderungen (siehe Seite 32).

Gehen Sie folgendermaßen vor:

1. Identifizieren Sie einen Host für den Domänen-Koordinationsrechner, der den Anforderungen entspricht.
2. Stellen Sie sicher, dass der Host für den Domänen-Koordinationsrechner über einen unterstützten JDK verfügt.

   Weitere Informationen finden Sie unter JDK-Voraussetzungen (siehe Seite 79).
3. Sie sollten planen, ob unterstützte Komponenten auf dem Host mit dem Domänen-Koordinationsrechner gespeichert werden sollen.

   Weitere Informationen finden Sie unter Planen der Speicherorte für unterstützenden Komponenten (siehe Seite 69).
4. Identifizieren Sie den Datenbankserver, um die Bibliotheks-, Berichts- und Laufzeitdatenbank für den Domänen-Koordinationsrechner zu hosten.
5. Bereiten sie den Datenbankserver vor.

   Weitere Informationen finden Sie unter Datenbankserver-Voraussetzungen (siehe Seite 71).
6. Identifizieren Sie den Host für CA EEM, wenn CA EEM nicht bereits mit einem anderen CA Technologies-Produkt verwendet wird.
7. Werten Sie Konfigurationsoptionen für CA EEM aus.

   Siehe Sie CA EE (siehe Seite 81)M-Voraussetzungen, einschließlich Voraussetzungen für das Konfigurieren von NTLM-Authentifizierung.

8. Wenn CA EEM mit CA SiteMinder konfiguriert ist, erwägen Sie, CA Process Automation für die Verwendung der SSO-Funktion zu konfigurieren.

   Weitere Informationen finden Sie unter So verwenden Sie CA SiteMinder mit CA Process Automation (siehe Seite 223).

9. Richten Sie optional einen Lastenausgleich ein, wenn Sie bereits wissen, dass der Domänen-Koordinationsrechner zu einem späteren Zeitpunkt geclustert werden muss. Weitere Informationen finden Sie unter Einrichten eines Lastenausgleichs für Koordinationsrechner-Clustering (siehe Seite 35).

10. Notieren Sie das Zertifikatskennwort, das Sie im Feld "Zertifikatskennwort" für den Domänen-Koordinationsrechner festlegen möchten, und bewahren Sie es an einem sicheren Ort auf.

    Wichtig! Sie müssen dieses gleiche Kennwort angeben, wenn Sie andere Koordinationsrechner oder zusätzliche Koordinationsrechner-Knoten installieren. Wenn Sie dieses Kennwort vergessen, müssen Sie jeden Koordinationsrechner in Ihrem System neu installieren, beginnend mit dem Domänen-Koordinationsrechner. Wenn Sie ein Upgrade auf eine neue Version durchführen, wird dasselbe Kennwort benötigt.

Planen der Speicherorte für die unterstützenden Komponenten

Ein Schritt in der Planung eines CA Process Automation-Systems besteht darin, zu bestimmen, welche neuen Komponenten auf dem Host des CA Process Automation-Domänen-Koordinationsrechner installiert werden können und welche auf separaten Hosts installiert werden müssen. Die Komponenten des CA Process Automation-Netzwerk werden nun genauer betrachtet.

- JDK: Muss gemeinsam installiert werden
- CA Embedded Entitlements Manager (CA EEM): Kann gemeinsam installiert werden, wird allerdings nicht empfohlen
- Datenbankserver für die CA Process Automation-Datenbanken: gemeinsam installiert werden, wird allerdings nicht empfohlen
- Lastenausgleich (wenn Clustering geplant ist): Kann nicht gemeinsam installiert werden
- Andere Koordinationsrechner: Können nicht gemeinsam installiert werden
- Cluster-Knoten: Können nicht gemeinsam installiert werden
- NTP-Server: Extern zum Netzwerk
- CA SiteMinder (optional): Kann gemeinsam installiert werden, dies wird allerdings nicht empfohlen

Cluster-Knoten und Koordinationsrechner werden normalerweise jeweils auf einem separaten Host installiert. Der NTP-Server kann für das Netzwerk extern sein.

Wenn CA Process Automation wenig ausgelastet ist, können Sie folgende Entitäten auf demselben Host installieren, auf dem Sie den Domänen-Koordinationsrechner installiert haben:

- CA EEM.
- Datenbankserver für die Bibliotheks-, Berichts- und Laufzeitzeitdatenbank.

Berücksichtigen Sie folgende Faktoren, wenn Sie bestimmen, ob Entitäten gemeinsam installiert werden können oder ob mehrere Hosts verwendet werden sollen:

- Eigenschaften des Host

  Größere Faktoren sind die Menge und die Geschwindigkeit der CPUs, der Speicherkapazität, des Festplattenspeichers und der Netzwerke.

- Volumen der Prozesse.

  Bedenken Sie nicht nur die Gesamtanzahl der Prozesse, sondern auch die maximalen dauerhaften Raten für Zeiträume mit hoher Auslastung.

- Prozessimplementierung.

  Nicht alle Prozesse sind gleich. Einige Prozesse haben wenige Operatoren, andere haben Hunderte. Einige Prozesse enthalten viele CPU-intensive Aktivitäten, während andere Prozesse die meiste Zeit auf Events oder Anwenderinteraktionen warten. Diese Unterschiede machen es schwierig das Laden hinsichtlich des Prozessvolumens bzw. der Prozessraten anzugeben. Sogar bei feinerer Granularität von Operatoren ist der Durchsatz unterschiedlich.

- Erforderliche Ebene der Reaktionsfähigkeit.

  Reaktionsfähigkeit in Echtzeit kann mit der aktuellen Implementierung niemals erreichbar werden. Allerdings müssen sogar weniger strenge Anforderungen berücksichtigt werden, wenn mehr Hardware für zusätzliche Koordinationsrechner eine Rolle spielt. Mit einem strengen SLA benötigt das System mehr freie Speicherkapazität, sodass die Zeiträume mit hoher Auslastung noch gut ausgeführt werden können. Ohne ein SLA benötigt das System nur ausreichende Kapazität, um die durchschnittliche Ladung abzudecken.

- Intensität der Verwendung für gemeinsame Komponenten.

  Überlegen Sie, wofür Sie CA EEM und das RDBMS sonst noch verwendet werden.

Im Hinblick auf zukünftiges Wachstum, wird empfohlen, CA EEM und den Datenbankserver mit dem Domänen-Koordinationsrechner nicht gemeinsam zu installieren. Sie können nur feststellen, ob Sie über genügend Ressourcen verfügen, wenn Sie die tatsächliche vollständige Auslastung testen.

Datenbankserver-Voraussetzungen

Für CA Process Automation ist es erforderlich, dass Sie über mindestens einen der folgenden Datenbankserver von Drittanbietern verfügen, auf dem CA Process Automation Daten speichern und dauerhaft aufbewahren kann:

- MySQL Server r5.5
- Microsoft SQL Server 2005, 2008, 2008 R2, 2012
- Oracle Database 10g Release 2 oder 11g Release 2

CA Process Automation verwendet drei Datenbanken. Diese Datenbanken können sich au demselben Datenbankserver, auf unterschiedlichen Datenbankservern desselben Typs oder auf Datenbankservern unterschiedlicher Typen befinden.

Wenn Sie einen dieser Server noch nicht eingerichtet haben, lesen Sie die entsprechenden Voraussetzungen, bevor Sie ihn einrichten. Es wird empfohlen, dass sich dieser Server und CA Process Automation auf separaten Hosts befinden.

Befolgen Sie die Richtlinien für den Datenbankservertyp, den Sie für diese Koordinationsrechner-Installation verwenden.

- Vorbereiten von MySQL Server für CA Process Automation (siehe Seite 74).
- Vorbereiten von Microsoft SQL Server für CA Process Automation (siehe Seite 75).
- Vorbereiten eines Oracle-Datenbankservers für CA Process Automation. (siehe Seite 77)

Informationen zu CA Process Automation-Datenbanken

Jeder Koordinationsrechner benötigt drei logische Datenbanken:

- Die Repository-Datenbank oder die *Bibliotheksdatenbank* ist eine Datenbank, die die Automatisierungsobjekte speichert, die in Ordnern auf der Registerkarte "Bibliothek" in CA Process Automation erstellt wurden. Zu den gespeicherten Daten gehören die Baumstruktur der Bibliothek, die vollständige Definition von jedem Objekt sowie Eigentümer- und Versionsinformationen.

  Hinweis: Mehrere Koordinationsrechner können die Repository-Datenbank auf dem Domänen-Koordinationsrechner gemeinsam nutzen oder jeder Koordinationsrechner kann seine eigene Repository-Datenbank haben.

- Die *Laufzeitdatenbank* ist eine Koordinationsrechner-spezifische Datenbank, in der Daten von Prozessinstanzen für einen einzelnen Koordinationsrechner oder Koordinationsrechner-Cluster gespeichert werden. Zu den Daten gehören Informationen über gegenwärtig ausgeführte Prozessinstanzen, Instanzen, die ausgeführt aber noch nicht in die Archivtabelle verschoben wurden und archivierte Instanzen. Sie können über die Registerkarte "Vorgänge" auf aktuelle und archivierte Daten zugreifen. Jeder Laufzeitdatensatz enthält den Zustand, den Datensatz und den Verantwortlichen für die Objektinstanz sowie die Ablaufplanungsinformationen.

  Hinweis: Jeder Koordinationsrechner benötigt eine getrennte Laufzeitdatenbank. Ein eigenständiger Koordinationsrechner verfügt über eine eigene Datenbank. Ein Koordinationsrechner-Cluster wird als eigenständiger logischer Koordinationsrechner behandelt. In diesem Fall verwenden alle Knoten dieselbe Datenbank.

- In der *Berichtsdatenbank* werden Verlaufsdaten für Prozess- und Operatorinstanzen gespeichert. Administratoren können mit diesen Daten Berichte fast in Echtzeit generieren, indem vordefinierte Berichtsdefinitionen und anwenderspezifische Berichtsdefinitionen auf der Registerkarte "Berichte" verwendet werden.

  Hinweis: Die Berichtsdatenbank wird normalerweise von allen Koordinationsrechnern gemeinsam genutzt.

Diese logischen Datenbanken können gemeinsam eine physische Datenbank nutzen. Als Best Practice sollten allerdings separate Datenbanken verwendet werden. CA Process Automation erfordert, dass in Datenbanken nicht zwischen Groß- und Kleinschreibung unterschieden wird.

Es wird ein Speicherplatz von mindestens 40 GB für Ihre Datenbanken empfohlen. Bestimmte Vorgänge, wie z. B. CA Process Automation-Upgrade durchführen, führen zu ungewöhnlich großen Anforderungen. Es ist empfehlenswert, immer genügend Speicherplatz bereitzustellen und den Speicherplatzverbrauch regelmäßig zu überwachen.

Hinweise zu Archivierungsrichtlinien

- Laufzeitdatenbanken erfahren während der Ausführung von Prozessen einen Zuwachs. Der erforderliche Speicherplatz zum Speichern dieser Daten hängt von der Größe des Inhalts der Prozessinstanz und von den Einstellungen der CA Process Automation-Archivierungsrichtlinie ab.
- Die Speicherung der Prozessinstanzen basiert auf der Archivierungsrichtlinie. Sie können die Richtlinie für die Archivbereinigung für folgende Aktionen konfigurieren:
  - Instanzen nach Ablauf eines bestimmten Zeitraums ins Archiv verschieben.
  - Ältere Instanzen automatisch löschen, ohne sie ins Archiv zu verschieben.
  - Keine Aktion durchführen.

    Hinweis: Wenn in der Richtlinie festgelegt ist, dass keine Aktion durchgeführt werden soll, wird empfohlen, außerhalb von CA Process Automation Datenarchivierungsaufgaben auszuführen.
- Die Archivierungsrichtlinie ist Koordinationsrechner-spezifisch.

Hinweis: Weitere Informationen finden Sie unter Konfigurieren der Koordinationsrechner-Richtlinien im *Handbuch für Inhaltsadministratoren*.

Weitere Informationen:

Erweiterte Konfigurationsoptionen (siehe Seite 21)

Vorbereiten von MySQL Server für CA Process Automation

Während der Installation des Domänen-Koordinationsrechners oder eines zusätzlichen Koordinationsrechners erstellt das Installationsprogramm CA Process Automation-Datenbanken im angegebenen MySQL-Server. Für das Installationsprogramm sind folgende Voraussetzungen zu erfüllen:

- Navigieren Sie während der Installation zum MySQL JDBC-Treiber. Diese Treiber ist nicht auf dem CA Process Automation-Installationsdatenträger enthalten.

  Hinweis: Wir empfehlen, Version 5.1.7 oder höher des MySQL JBDC-Treibers zu verwenden.
- Anmeldeinformationen mit Verwaltungsberechtigungen, um die Bibliotheks-, Berichts- und Laufzeitdatenbanken zu erstellen.
- Zwei für CA Process Automation angepasste MySQL-Variablen.

Bevor Sie einen Koordinationsrechner installieren, der den MySQL-Datenbankserver verwendet, bereiten Sie den MySQL-Server für CA Process Automation vor.

Gehen Sie folgendermaßen vor:

1. Laden Sie den JDBC-Treiber von der MySQL-Website herunter. Laden Sie zum Beispiel MySQL Connector/J 5.1.7 herunter.
2. Speichern Sie den Treiber an einem Speicherort, zu dem Sie während der Installation navigieren können.
3. Öffnen Sie MySQL Workbench, und wählen Sie unter "Konfiguration" die Optionsdatei aus.
4. Legen Sie die Variable für den Zeitraum fest, die eine Transaktion auf eine Sperre wartet, bevor sie rückgängig gemacht wird:
   a. Wählen Sie die Registerkarte "InnoDB" aus.
   b. Führen Sie einen Bildlauf zur Gruppe "Verschiedene" durch.
   c. Wählen Sie "innodb_lock_wait_timeout" aus.
   d. Ändern Sie den Standardwert 50 in einen Wert, der größer als 60 ist.

      ```
      innodb_lock_wait_timeout = 90
      ```

5. Legen Sie die größtmögliche Paketlänge auf 33554432 Byte (32 MB) fest, die dem Server gesendet und von diesem empfangen werden kann. Die Standardwert beträgt 1048576.
   a. Wählen Sie die Registerkarte "Netzwerk" aus.
   b. Suchen Sie die Gruppe "Daten" bzw. "Speicher".
   c. Wählen Sie "max_allowed_packet" aus.
   d. Geben Sie den erforderlichen Wert ein.
6. Klicken Sie auf Anwenden.

   Eine Bestätigung der Änderungen, die für die MySQL-Konfigurationsdatei übernommen werden, wird angezeigt.

Vorbereiten von Microsoft SQL Server für CA Process Automation

Bevor Sie den CA Process Automation-Domänen-Koordinationsrechner oder einen zusätzlichen Koordinationsrechner installieren, bei dem sich die CA Process Automation-Datenbanken auf SQL Server befinden, führen Sie die folgenden Aufgaben aus:

- Stellen Sie sicher, dass SQL Server den CA Process Automation-Anforderungen entspricht (siehe Seite 76).
- Verstehen Sie, wie der JDBC 3.0-Treiber referenziert wird (siehe Seite 76).
- Überprüfen Sie die Richtlinien für das Angeben des Datenbankservernamens für SQL Server (siehe Seite 77).

Stellen Sie sicher, dass SQL Server den CA Process Automation-Anforderungen entspricht

Wenn Sie SQL Server für CA Process Automation vorbereiten, müssen die Datenbanken folgende Anforderungen erfüllen:

- SQL Server muss mit Authentifizierung im gemischten Modus installiert oder konfiguriert werden. Sie geben während der Installation des Koordinationsrechners ein Konto mit SQL Server-Authentifizierung an.
- Das Installationsprogramm des Domänen-Koordinationsrechners erfordert, dass Anwender-Anmeldeinformationen mit Verwaltungsberechtigungen eingegeben werden, um die CA Process Automation-Datenbanken zu erstellen.
- Die SQL Server-Sortierung für CA Process Automation-Datenbanken muss "SQL_Latin1_General_CP1_CI_AS" sein. Standardmäßig erstellt das CA Process Automation-Installationsprogramm Datenbanken mit dieser Sortierung.

Prüfen Sie die Konfigurationsdatei für Ihren SQL Server, um sicherzustellen, dass Ihr SQL Server die CA Process Automation-Anforderungen erfüllt.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu der Datei "ConfigurationFile.ini", die in einem Pfad erstellt wird, der ungefähr folgendermaßen aussieht:

   ```
   C:\ Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\ yyyymmdd_hhmmss
   ```

2. Stellen Sie sicher, dass die Einstellung des Sicherheitsmodus ungefähr so aussieht:

   ```
   ; The default is Windows Authentication. Use "SQL" for Mixed Mode Authentication.

   SECURITYMODE="SQL"
   ```

3. Stellen Sie sicher, dass die Einstellung für die Anmeldeinformationen für das SQL-Systemadministratorkonto ungefähr so aussieht:

   ```
   ; Windows account(s) to provision as SQL Server system administrators.
   SQLSYSADMINACCOUNTS=".\Administrator"
   ```

4. Stellen Sie sicher, dass die Einstellung für die Sortierung ungefähr so aussieht:

   ```
   ; Specifies a Windows collation or an SQL collation to use for the Database Engine.
   SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
   ```

So wird der JDBC-Treiber JTDS referenziert

Während der Installation des Koordinationsrechners benötigt das Installationsprogramm den JTDS 1.3-Treiber für SQL Server. Er befindet sich auf DVD1. Der Pfad ist:

```
.../DVD1/drivers/jtds-1.3.jar
```

Richtlinien für das Angeben des Datenbankservernamens für SQL Server

Wenn Sie den Domänen-Koordinationsrechner oder einen nicht geclusterten Koordinationsrechner installieren, dann geben Sie Details für drei CA Process Automation-Datenbanken an: Bibliothek, Laufzeit und Berichterstellung. Wenn Sie in "Typ der Datenbank" "MS SQL" angeben, verwenden Sie folgende Richtlinien, um den Datenbankserver anzugeben:

- Wenn Sie nur eine SQL Server-Instanz auf dem Hostserver haben, geben Sie den Hostnamen des Servers an. (Dieser Name ist die Standardinstanz.)
- Wenn Sie mehrere SQL Server-Instanzen auf dem Hostserver haben, geben Sie die Instanz mit dem Namen "SQL Server" im Format *host_name**named_instance* an.

  Eine Instanz mit dem Namen "SQL Server" ist eine weitere Kopie von SQL Server, die auf dem gleichen Host ausgeführt wird. Jede Kopie wird unabhängig ausgeführt, und jede Kopie wird über den Instanzennamen unterschieden. Ein Datenbankserver kann viele benannte Instanzen jedoch nur eine Standardinstanz (unbenannt) haben.

Vorbereiten von Oracle-Datenbankservern für CA Process Automation

Bevor Sie den Domänen-Koordinationsrechner oder einen zusätzlichen Koordinationsrechner, der Oracle als Host für seine internen Datenbanken verwendet, installieren, sind Vorbereitungsschritte erforderlich.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie einen Anwender mit Verbindungs- und Ressourcenberechtigungen.
2. Stellen Sie sicher, dass Oracle über ausreichend Tablespace verfügt, um folgende Datenbanken zu hosten:
   - Bibliotheksdatenbank
   - Laufzeitdatenbank
   - Berichtsdatenbank

3. Erstellen Sie die Bibliotheks-, Berichtes- und Laufzeitdatenbanken manuell.
4. Konfigurieren Sie folgende Einstellungen:
   - Legen Sie die maximalen Verbindungen auf 100 fest (oder mindestens 150 für geclusterte Koordinationsrechner).

     Alle Verbindungen werden durch Koordinationsrechner hergestellt, aber für ein optimales Verhalten werden einige zusammengefasste Verbindungen benötigt.
   - Legen Sie "Online Transaction Processing (OLTP)" fest, um Transaktionen zu vereinfachen.
5. Sie sollten verstehen, wie der Oracle JDBC-Treiber referenziert wird.

   Während der Installation des Koordinationsrechners benötigt das Installationsprogramm den Oracle JDBC-Treiber für Oracle, der sich auf DVD1 befindet. Der Pfad ist:

   ```
   .../DVD1/drivers/ojdbc14.jar
   ```

Hinweise:

- Partitionierung wird *nicht* unterstützt.

Privilegien des Verantwortlichen für die Datenbank

Wenn Sie CA Process Automation erstmals oder nach der Anwendung eines Patches starten, überprüft die Anwendung die Datenbank- oder Schemastruktur und passt sie an.

Die minimalen Datenbankberechtigungen, die CA Process Automation benötigt, lauten:

- Zugriffsrechte für Metadaten (für die Ermittlung der Struktur)
- Berechtigungen zum Erstellen, Ändern und Verwerfen (create/alter/drop, CAD) von DDLs für Tabellen, Indizes, Ansichten, Einschränkungen und Sequenzen in der Datenbank.
- Lese- oder Schreibberechtigungen für alle Tabellen

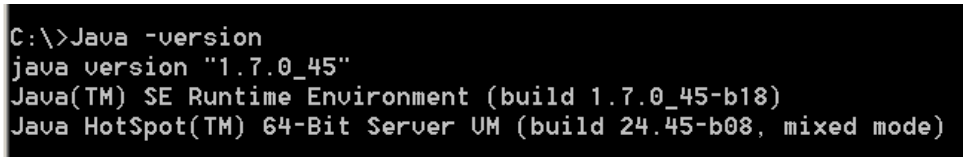
Die CA Process Automation-Anwendung benötigt die folgenden Berechtigungen für ihre Tabellen:

- Auswahl
- Einfügen
- Löschen

JDK-Voraussetzungen

Bevor Sie einen Koordinationsrechner installieren, stellen Sie sicher, dass die Voraussetzungen des Java Development Kit (JDK) erfüllt werden. Verwenden Sie folgenden Befehl:

```
Java -version
```


C:\>Java -version
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b18)
Java HotSpot(TM) 64-Bit Server VM (build 24.45-b08, mixed mode)

Das vorhergehende Beispiel veranschaulicht eine gültige Java-Version für Windows.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei jenem Host an, auf dem Sie den Domänen-Koordinationsrechner installieren möchten.
2. Stellen Sie sicher, dass es sich bei Ihrem Java Development Kit um Oracle JDK 1.7 handelt.

   Hinweis: Weitere Details finden Sie unter Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30). Wenn sich die Java-Standardversion unterscheidet, ändern Sie die standardmäßige Java-Version in der Shell, wo Sie das CA Process Automation-Installationsprogramm starten werden.
3. Wenn die erforderliche JDK-Version nicht installiert ist, laden Sie sie von der Oracle-Website herunter, und führen Sie den Installationsassistenten aus, um den JDK zu installieren.
4. Stellen Sie bei geclusterten Koordinationsrechnern sicher, dass Oracle JDK auf allen Knoten installiert ist.

Festlegen des standardmäßigen Java-Homepfads

Wenn sich die Standardversion unterscheidet, ändern Sie die standardmäßige Java-Version auf der Shell, wo Sie die CA Process Automation-Installation starten werden.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zum Ordner "DVD1".
2. Legen Sie die standardmäßige Java-Einstellung an der Eingabeaufforderung oder der Shell fest.

   Windows

   ```
   set JAVA_HOME=<home_directory_of_jdk (not_bin)>
   set PATH=%JAVA_HOME%\bin;%PATH%
   ```

   UNIX oder Linux

   ```
   export JAVA_HOME=<home_directory_of_jdk (not_bin)>
   export PATH=$JAVA_HOME/bin:$PATH
   ```

3. Starten Sie das Installationsprogramm an dieser Eingabeaufforderung oder von dieser Shell.

   Windows

   ```
   .\ Domain_Installer_windows.bat
   ```

   UNIX oder Linux

   ```
   ./ Domain_Installer_unix.sh
   ```

   Das Installationsprogramm startet zuerst das Installationsprogramm für Drittanbietersoftware und danach das Installationsprogramm für den Domänen-Koordinationsrechner.

CA EEM-Voraussetzungen

CA Process Automation verwendet CA Embedded Entitlements Manager (CA EEM) für die Anwenderauthentifizierung und -autorisierung. CA EEM ist eine benötigte Voraussetzung.

- Wenn Sie CA EEM mit einem anderen CA Technologies-Produkt verwenden, überprüfen Sie, ob es sich dabei um eine von CA Process Automation unterstützte Version handelt. Weitere Informationen finden Sie unter Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
- Wenn Sie nicht über CA EEM verfügen oder wenn Ihr CA EEM eine frühere Version ist als die Versionen, die CA Process Automation unterstützt, dann sollten Sie CA EEM herunterladen und installieren (siehe Seite 82).
- Planen Sie, wie Sie CA Process Automation-Anwender authentifiziert werden sollen (siehe Seite 88).
- Sammeln Sie CA EEM-bezogene Informationen für die Installation des Domänen-Koordinationsrechners (siehe Seite 84).
- Um während der Installation zwei CA EEM-Instanzen zu erstellen (eine, mit der Sie arbeiten und die andere als Backup für ein Failover), lesen Sie den Abschnitt Vorbereiten für ein Failover auf einen Backup-CA EEM (siehe Seite 83). Dieser Vorgang ist optional und kann zu einem späteren Zeitpunkt ausgeführt werden.

Einrichten von CA EEM

CA Process Automation benötigt CA EEM für die Verwaltung von Autorisierung und Authentifizierung. Vor einer Installation oder einem Upgrade von CA Process Automation muss eine geeignete CA EEM-Instanz verfügbar sein. CA Process Automation kann eine beliebige Version von CA EEM 8.4 SP04 CR10 bis 12.5.1 verwenden. Manche CA EEM-Funktionen, die von CA Process Automation verwendet werden können, werden jedoch nicht in allen CA EEM-Versionen unterstützt. Zum Beispiel:

Für die Unterstützung von 2048- und 4096-Bit-Sicherheitszertifikaten ist Version 12.0 oder höher von CA EEM erforderlich.

Für die Unterstützung von mehreren Microsoft Active Directory-Domänen ist Version 12.5 oder höher von CA EEM erforderlich.

Wenn Ihr Standort über eine vorhandene CA EEM-Instanz verfügt, die nicht der erforderlichen Version entspricht, beraten Sie sich mit Ihrem Standortadministrator, um festzustellen, ob ein Upgrade der CA EEM-Instanz auf die gewünschte Ebene durchgeführt werden kann. Einschränkungen der Versionsunterstützung für andere Produkte, die die CA EEM-Instanz verwenden, können dem Upgrade der Instanz möglicherweise im Wege stehen.

Neue CA EEM-Installation

Eine neue CA EEM-Installation ist erforderlich, wenn keine CA EEM-Instanz verfügbar ist, die der gewünschten Version entspricht.

Gehen Sie folgendermaßen vor:

Laden Sie die Installationsprogramme für CA EEM 12.5.1 vom Speicherort der CA Process Automation-Installationsdatenträger herunter.

Folgen Sie den Anweisungen der CA EEM-Dokumentation, wenn Sie Ihre CA EEM-Instanz bereitstellen oder ein Upgrade durchführen.

Hinweise zur CA EEM-Konfiguration

Wenn Sie CA EEM für die Verwendung des internen oder eines externen Anwenderspeichers konfigurieren, berücksichtigen Sie die folgenden Auswirkungen auf CA Process Automation:

Wenn Sie den standardmäßigen internen Anwenderspeicher auswählen, können Sie Anwenderkonten für CA Process Automation-Anwender erstellen. Bei der Anmeldung werden für die Authentifizierung Anwender-Anmeldeinformationen verwendet, die in CA EEM definiert sind.

Wenn Sie auf einen externen Anwenderspeicher verweisen, werden Anwenderkonten aus jenem Speicher automatisch in CA EEM als globale Anwender geladen. Für die Authentifizierung werden Anwender-Anmeldeinformationen verwendet, die im referenzierten Microsoft Active Directory-Verzeichnis definiert sind.

Siehe Referenz von globalen Anwendern und globalen Gruppen von Microsoft Active Directory (siehe Seite 93). (CA EEM 8.4)

Weitere Informationen finden Sie unter Referenz von globalen Anwendern aus mehreren Active Directorys (siehe Seite 93). (CA EEM 12.51)

Wenn Sie CA EEM für die Verwendung im FIPS-Modus konfigurieren, beachten Sie folgende Faktoren:

CA Process Automation verschlüsselt die Daten, die zwischen CA Process Automation und CA EEM transportiert werden.

Wenn der FIPS-Modus in CA EEM aktiviert ist, muss CA Process Automation so konfiguriert sein, dass für die Kommunikation zwischen CA Process Automation und CA EEM Algorithmen, die von FIPS unterstützt werden, verwendet werden können. Wählen Sie bei der Installation von CA Process Automation "FIPS-konformes Zertifikat verwenden" aus, um von FIPS unterstützte Algorithmen zu verwenden.

Vorbereiten für ein Failover auf einen Backup-CA EEM

Sie sollten es in Betracht ziehen, zwei CA EEM-Instanzen in einer Hochverfügbarkeitskonfiguration einzurichten. Wenn CA EEM auf diese Weise konfiguriert ist, dient die primäre CA EEM-Instanz als aktiver Sicherheitsauthentifizierungsserver und Sicherheitsautorisierungsserver für CA Process Automation. Die sekundäre CA EEM-Instanz dient als Backup für Sicherheitsauthentifizierungsserver und Sicherheitsautorisierungsserver. Der sekundäre CA EEM spiegelt den primären CA EEM. Die beiden CA EEM-Instanzen können auf das gleiche externe Verzeichnis verweisen.

CA Process Automation führt automatisch und transparent ein Failover vom primären CA EEM zum sekundären CA EEM durch, wenn der primäre CA EEM fehlschlägt, nachdem CA Process Automation die anfängliche Verbindung herstellt. Ein Failover wird durchgeführt, auch wenn der primäre Server anfänglich ausgeschaltet ist, wenn Sie beide CA EEM-Server in CA Process Automation konfigurieren.

Weitere Informationen finden Sie in der CA EEM-Dokumentation für die CA EEM-Version, die an Ihrem Standort bereitgestellt wird und Informationen über das Einrichten von CA EEM in einer Hochverfügbarkeitskonfiguration enthält. Zusätzliche Informationen sind auf der Seite mit den Best Practices für die CA Process Automation-Implementierung verfügbar (zugänglich über einen Quicklink auf der Registerkarte "Startseite" von CA Process Automation).

Sammeln von CA EEM-bezogenen Informationen für die Installation des Domänen-Koordinationsrechners

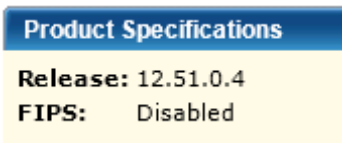
Bevor Sie mit der Installation des Domänen-Koordinationsrechners beginnen, sollten Sie folgende Details Ihrer CA EEM-Konfiguration bereithalten:

- Die CA EEM-Admin-Anmeldeinformationen, wobei "EiamAdmin" der Anwendername ist.
- Die CA EEM-Release-Version und die FIPS-Einstellung in CA EEM.

  1. Navigieren Sie zum von Ihnen verwendeten CA EEM.

     `https://server:5250/spin/eiam`

  2. Wählen Sie den CA Process Automation-Anwendungsnamen aus der Drop-down-Liste der Anwendungen aus.
  3. Geben Sie gültige Anmeldeinformationen (**EiamAdmin**) und das zugehörige Kennwort ein. Klicken Sie auf "Anmeldung".
  4. Klicken Sie "Info". Die CA EEM-Release-Version und die FIPS-Einstellung werden unter "Produktspezifikationen" angezeigt.



Hinweis: Während der CA Process Automation-Installation generiert der Prozess, der auch die CA Process Automation-Anwendung mit CA EEM registriert, die Zertifikate, die CA Process Automation verwendet, um eine Verbindung zu CA EEM herzustellen.

- Wenn CA EEM FIPS-aktiviert ist, dann werden sowohl "PAM.cer" als auch "PAM.key" generiert.
- Wenn CA EEM für FIPS deaktiviert ist, geben Sie ein Kennwort (das EEM-Zertifikatskennwort) an, bevor Sie die CA Process Automation-Anwendung mit CA EEM registrieren. Dieses Kennwort wird in weiterer Folge verwendet, um das PAM.p12-Zertifikat zu schützen, das generiert wird, wenn die CA Process Automation-Anwendung mit CA EEM registriert wird.
- Wenn Sie eine Installation *ohne Registrierung* der CA Process Automation-Anwendung mit CA EEM durchführen, werden Sie aufgefordert, den SDK entsprechend der Version Ihres CA EEM-Servers auszuwählen.

- Der Hostname des CA EEM-Servers. Um den Hostnamen zu bestimmen, melden Sie sich bei CA EEM an. Der Hostname wird mit der Bezeichnung "Backend" in der Titelleiste angezeigt.

  Wichtig! Sie benötigen das EiamAdmin-Kennwort, um sich bei CA EEM anzumelden.

- Wenn Sie ein Upgrade durchführen und CA EEM für die Verwendung von mehreren Microsoft Active Directory-Verzeichnissen konfigurieren möchten, müssen Sie den Namen des AD-Verzeichnisses, das Sie derzeit referenzieren, kennen. Sie sollten diese Domäne als standardmäßige AD-Domäne angeben. CA Process Automation-Anwender, die zur standardmäßigen Domäne gehören, können sich mit ihrem nicht vollständig qualifizierten Anwendernamen bei CA Process Automation anmelden, nachdem Sie sie neu zu einer Anwendungsgruppe zugewiesen haben.
- Notieren Sie das Zertifikatskennwort, das Sie eingeben werden. Dieses Zertifikatskennwort steuert den Zugriff auf die Schlüssel, die zum Verschlüsseln der Kennwörter und anderer kritischer Daten verwendet werden. Das Zertifikatskennwort ist einer einzelnen CA Process Automation-Domäne eigen. (Dieses Zertifikatskennwort ist nicht CA EEM-spezifisch, doch es ist wichtig, dass Sie es notieren.)

  Wichtig! Sie müssen dasselbe Kennwort verwenden, wenn Sie einen anderen Koordinationsrechner installieren oder Cluster-Knoten zu einem Koordinationsrechner hinzufügen. Dasselbe Kennwort ist eine erforderliche Eingabe, wenn Sie ein Upgrade von CA Process Automation durchführen.

Identifizieren der Version des von CA Process Automation verwendeten CA EEM-SDK

Sie können feststellen, ob das CA EEM SDK, das CA Process Automation verwendet, SDK-Version 8 oder SDK-Version 12 ist.

Gehen Sie folgendermaßen vor:

1. Stoppen Sie den Domänen-Koordinationsrechner
2. Vergrößern Sie die Protokollebene des Domänen-Koordinationsrechners auf "INFO".
3. Starten Sie den Domänen-Koordinationsrechner.
4. Melden Sie sich beim CA Process Automation-Server an.
5. Überprüfen Sie die Protokolle.
   - Wenn CA Process Automation CA EEM-SDK r8.4 verwendet:

     ```
     13:03:16.859 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByUserName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     8
     13:03:16.861 INFO
     [com.optinuity.c2o.eemconfiguration.EEM8Manager]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM8Manager...
     ```

   - Wenn CA Process Automation CA EEM SDK 12.51 verwendet:

     ```
     13:32:37.195 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByPrincipalName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     12
     13:32:37.198 INFO
     [com.optinuity.c2o.eemconfiguration.EEM12Manager]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM12Manager...
     ```

6. Halten Sie den Domänen-Koordinationsrechner an, setzen Sie die Einstellung der Protokollebene auf die vorherige Ebene zurück, und starten Sie anschließend den Domänen-Koordinationsrechner neu.

Voraussetzungen für das Konfigurieren von NTLM-Authentifizierung

Gehen Sie folgendermaßen vor, bevor Sie die NTLM-Authentifizierung konfigurieren:

- Stellen Sie sicher, dass CA EEM auf einem Server mit einem Microsoft Windows-Betriebssystem installiert ist.
- Stellen Sie sicher, dass CA EEM Microsoft Active Directory als externen Anwenderspeicher verwendet.
- Stellen Sie sicher, dass CA EEM nicht für mehrere Active Directorys oder für eine Active Directory-Gesamtstruktur konfiguriert ist.
- Stellen Sie sicher, dass Anwender über Windows-Computer zu CA Process Automation navigieren.
- Stellen Sie sicher, dass der CA EEM-Server und der Computer, von dem Anwender zu CA Process Automation navigieren, zur gleichen Netzwerkdomäne gehören. Wenn die Computer zu geschachtelten Domänen gehören, stellen Sie sicher, dass der CA EEM-Server und der Computer, auf dem die Anwendung gestartet wird, zu Domänen gehören, zwischen denen eine Vertrauensstellung besteht.
- Stellen Sie sicher, dass die Domänenanwender zu den Anwendergruppen auf dem Computer hinzugefügt sind, auf dem die Anwendung gestartet wird.

Planen, wie CA Process Automation-Anwender authentifiziert werden

Wenn dies eine neue CA Process Automation-Installation ist, dann wird als Teil der Vorbereitung festgelegt, wie CA Process Automation-Anwender authentifiziert werden sollen. Das tatsächliche Setup, das hier beschrieben wird, wird durchgeführt, nachdem die Installation fertiggestellt ist. Allerdings basieren die von Ihnen aktivierten CA Process Automation-Installationsoptionen auf Ihren Plänen. Es sind folgende Optionen verfügbar:

- Erstellen Sie für jeden CA Process Automation-Anwender in CA EEM ein Anwenderkonto. Der CA EEM-Administrator weist jedem Konto eine Anwender-ID zu. Anwender können ihre Kennwörter in CA EEM ändern. CA EEM authentifiziert Anwender, die sich bei CA Process Automation anmelden, indem verifiziert wird, ob die Angaben für Anwender-ID und Kennwort (die Anmeldeinformationen) zu einem aktiven Anwenderkonto gehören.
- Referenzierte Anwenderkonten, die in einem oder in mehreren Microsoft Active Directorys gespeichert sind. CA EEM übergibt die Anmeldeinformationen, die für die Anmeldung bei CA Process Automation verwendet werden, an AD. Die Authentifizierung wird in AD durchgeführt.
- Verwenden Sie NTLM-Authentifizierung (Pass-Through) ohne SiteMinder. Als Voraussetzung müssen die Anwenderkonten, auf die verwiesen wird, in einer einzigen Microsoft Active Directory-Domäne (AD-Domäne) gespeichert sein. NTLM-Authentifizierung wird nicht unterstützt, wenn Verweise auf mehrere Microsoft AD-Domänen vorliegen. Für NTLM-Authentifizierung ist es erforderlich, dass alle betroffenen Computer ein Windows-Betriebssystem verwenden und sich in derselben Domäne oder in Domänen mit Vertrauensstellung befinden.
- Aktivieren Sie Single Sign-On mithilfe von NTLM-Authentifizierung. Dafür muss CA SiteMinder verwendet oder den Voraussetzungen für das Konfigurieren von NTLM-Authentifizierung (siehe Seite 87) entsprochen werden. Wählen Sie in beiden Fällen während der Installation NTLM-Authentifizierung aus. Wenn Anwender zu CA Process Automation navigieren, wird die Authentifizierung von NTLM gehandhabt. Authentifizierte Anwender werden mit ihren Windows-Anmeldeinformationen angemeldet. Alternativ dazu können Sie NTLM-Pass-Through-Authentifizierung nach der Installation aktivieren (siehe Seite 135).

Bei einer Neuinstallation von CA Process Automation besteht ein Teil der Vorbereitung darin, zu entscheiden, wie CA Process Automation-Anwender authentifiziert werden sollen. Die hier beschriebenen Einrichtungsschritte werden nach Abschluss der Installation durchgeführt. Die ausgewählte Authentifizierungsmethode beeinflusst jedoch, welche Einstellungen bei der CA Process Automation-Installation angegeben werden müssen. Die Authentifizierungsoptionen umfassen Folgendes:

EEM-basierte Authentifizierung

- Systemeigener EEM-basierter Anwender

  Voraussetzungen

- Installation von CA EEM

  Details: Ein CA EEM-Administrator erstellt in CA EEM ein Anwenderkonto für jeden Anwender, der Zugriff auf CA Process Automation benötigt. Der CA EEM-Administrator stellt jedem Anwender eine Anmelde-ID zur Verfügung. Anwender können ihre Kennwörter in CA EEM ändern. CA EEM authentifiziert Anwender, die sich bei CA Process Automation anmelden, indem verifiziert wird, ob die Angaben für Anwender-ID und Kennwort (die Anmeldeinformationen) zu einem aktiven Anwenderkonto gehören.

Erforderliche Aktion während der Installation von CA Process Automation

Keine Aktion erforderlich

Verweis auf das LDAP-Verzeichnis

Voraussetzungen

Installation von CA EEM

Zugriff auf ein externes LDAP-basiertes Verzeichnis

Details: Die folgenden Verzeichnistypen und Konfigurationen sind verfügbar:

Active Directory (AD)

CA EEM kann konfiguriert werden, um auf Anwenderkonten zu verweisen, die in einem oder mehreren Microsoft Active Directory-Verzeichnissen gespeichert sind. CA Process Automation übergibt die Anmeldeinformationen an CA EEM, und CA EEM übergibt diese Anmeldeinformationen zur Validierung an AD.

LDAP-basiertes Verzeichnis, bei dem es sich nicht um AD handelt

CA EEM kann auch konfiguriert werden, um ein LDAP-basiertes Verzeichnis zu verwenden, bei dem es sich nicht um AD handelt. Die Authentifizierung wird in diesem Fall auf die gleiche Weise gehandhabt.

Erforderliche Aktion während der Installation von CA Process Automation

Keine Aktion erforderlich

Aktivieren von Single Sign-On mithilfe von NTLM-Authentifizierung

Voraussetzungen

Die Voraussetzungen sind mit jenen für AD oder LDAP-Verzeichnisse identisch.

(NEED TO VERIFY if NTLM authentication is not supported if you reference multiple Microsoft AD domains.)

Darüber hinaus müssen Sie in der Lage sein, die Voraussetzungen für die Konfiguration von NTLM-Authentifizierung zu erfüllen.

Hinweis: Eine Voraussetzung besteht darin, dass PAM-Anwender ein Windows-Betriebssystem verwenden und sich in einer einzigen Domäne oder in Domänen, für die eine Vertrauensstellung mit dem EEM-Server besteht, befinden.

Details: CA EEM führt die Authentifizierung über NTLM durch, wenn Anwender zu CA Process Automation navigieren. Authentifizierte Anwender werden mit ihren Windows-Anmeldeinformationen angemeldet.

Erforderliche Aktion während der Installation von CA Process Automation

Aktivieren Sie bei der Installation auf der Seite des EEM-Assistenten die NTLM-Option. Dies ist die empfohlene Methode zum Aktivieren von SSO.

Hinweis: Sie können NTLM-Pass-Through-Authentifizierung bei Bedarf nach der Installation aktivieren.

SiteMinder-basierte Authentifizierung

Single Sign-On mit CA SiteMinder

Voraussetzungen

[Point to SiteMinder doc]

Details: SiteMinder führt die Authentifizierung mit einem externen Verzeichnis durch und sendet den Anwendernamen an CA Process Automation. Anschließend wird der Anwender in CA EEM autorisiert. [We should probably point the user to the SiteMinder section in our install guide for more details.]

Erforderliche Aktion während der Installation von CA Process Automation

Hostname und Header für SiteMinder werden auf der Seite des Lastenausgleichsassistenten angegeben.

Authentifizierung und Autorisierung von Anwendern im FIPS-Modus

CA EEM kann für die Verwendung im FIPS-Modus konfiguriert werden. Dies ist eine Option. Damit CA Process Automation für FIPS konfiguriert werden kann, muss CA EEM für die Verwendung im FIPS-Modus konfiguriert sein. CA Process Automation kann auch ohne FIPS verwendet werden, wenn CA EEM für die Verwendung im FIPS-Modus konfiguriert ist.

Daten, die zwischen CA EEM und CA Process Automation übertragen werden, werden unabhängig davon, ob der FIPS-Modus aktiviert ist, verschlüsselt. Der Unterschied sind die verwendeten Algorithmen für die Verschlüsselung.

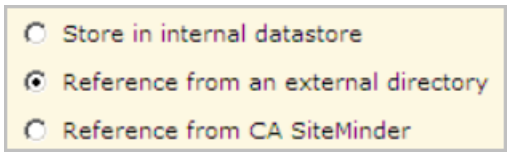
Wenn Anwender sich anmelden, überträgt CA Process Automation den Anwendernamen und Kennwort auf CA EEM. CA EEM gibt CA Process Automation Authentifizierungs- und Autorisierungsdaten zurück.

- Wenn FIPS-Modus aktiviert ist:
  - Übertragene Daten werden mit dem SHA1-Algorithmus verschlüsselt, der von FIPS unterstützt wird.
  - Ein PAM.cer-Zertifikat wird verwendet.
- Wenn FIPS-Modus deaktiviert ist:
  - Übertragene Daten werden mit dem MD5-Algorithmus verschlüsselt.
  - Ein PAM.p12-Zertifikat wird verwendet.

Bestimmen des CA EEM-Konfigurationstyps für das Speichern globaler Anwender

Beachten Sie beim Erfüllen der CA EEM-Voraussetzungen für eine Erstinstallation von CA Process Automation folgende Punkte:

- Ein Teil der CA EEM-Konfiguration besteht darin, auszuwählen, ob Anwender-Anmeldeinformationen intern gespeichert werden sollen, oder ob aus einem externen Verzeichnis oder von SiteMinder darauf verwiesen werden soll.



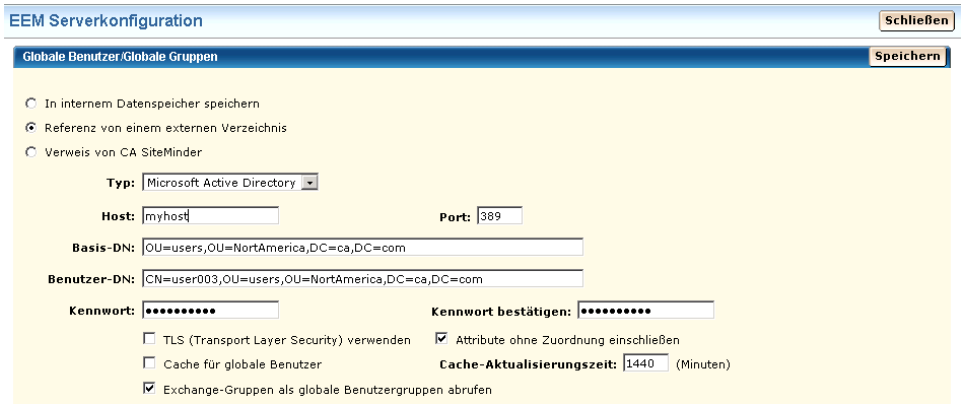
- Wenn Sie eine vorhandene CA EEM-Instanz verwenden, die neben CA Process Automation weitere Anwendungen unterstützt, sind diese Option und der Konfigurationstyp bereits definiert. Alle Anwendungen verwenden denselben Konfigurationstyp. Die Konfigurationstypen variieren je nach Version.
  - In Version 8.4 von CA EEM umfasst die Option "Referenz von einem externen Verzeichnis" den Konfigurationstyp "Microsoft Active Directory".
  - In Version 12.5 von CA EEM enthält die Option "Referenz von einem externen Verzeichnis" eine Reihe von Konfigurationstypen, einschließlich mehrere AD-Domänen und eine AD-Gesamtstruktur.
- Wenn Sie eine neue CA EEM-Instanz verwenden, ziehen Sie in Erwägung, den folgenden Vorgang zu verwenden:
  1. Installieren Sie CA EEM, und starten Sie CA EEM.
  2. Installieren Sie CA Process Automation. Registrieren Sie sich während der Installation mit CA EEM, sodass die CA Process Automation-Anwendung in CA EEM erstellt wird, und überspringen Sie den Test der Konnektivität mit CA EEM.
  3. Melden Sie sich mit den Anmeldeinformationen des EiamAdmin-Anwenders und dem CA Process Automation-Anwendungsnamen bei CA EEM an.
  4. Definieren Sie den Anwenderspeicher. Wenn Sie "Referenz von einem externen Verzeichnis" verwenden, definieren Sie die Details.

     Weitere Informationen zur Konfiguration von globalen Anwendern von einem referenzierten Anwenderspeicher in CA EEM finden Sie in der CA EEM-Dokumentation. Sehen Sie sich außerdem die folgenden Beispiele an:
     - Referenz von globalen Anwendern und globalen Gruppen von Microsoft Active Directory (siehe Seite 93) (CA EEM r8.4).
     - Referenz von globalen Anwendern von Microsoft Active Directorys (CA EEM r12.5) (siehe Seite 93)
  5. Konfigurieren Sie CA Process Automation-Anwender in CA EEM. Informationen finden Sie unter "Zuweisen einer Anwendungsgruppe zu einem globalen Anwender" im *Handbuch für Inhaltsadministratoren*.
  6. Optional können Sie CA EEM so konfigurieren, dass sich referenzierte Anwender mit ihrem E-Mail-Namen anmelden dürfen (siehe Seite 136).

Referenz von globalen Anwendern aus einem Microsoft Active Directory (CA EEM r8.4)

Wenn Sie CA EEM r8.4 installieren, können Sie die Option "Referenz von einem externen Verzeichnis" und anschließend "Microsoft Active Directory" als Typ auswählen.

Wenn Sie NTLM für Sicherheit verwenden, wählen Sie das Kontrollkästchen "Exchange-Gruppen als globale Benutzergruppen abrufen" wie im folgenden Beispiel aus:



Wenn Sie die Konfiguration speichern, werden folgende Statusmeldungen angezeigt:

- Externe Verzeichnisbindung erfolgreich.
- Externe Verzeichnisdaten geladen.

Wenn NTLM aktiviert ist und ein globaler Anwender sich das erste Mal anmeldet, wird in einem Dialogfeld angezeigt, das eine Authentifizierung erforderlich ist. CA EEM verwendet dann das NTLM-Protokoll, um Anwender zu authentifizieren.

Referenz von globalen Anwendern von Microsoft Active Directorys (CA EEM 12.5)

Wenn Sie CA EEM r12.51 installieren, können Sie CA EEM für Verweise auf mehrere Microsoft Active Directory-Verzeichnisse oder eine Active-Directory-Gesamtstruktur konfigurieren.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als EiamAdmin-Anwender in CA EEM an. Geben Sie als Anwendung <Global> an.
2. Klicken Sie auf die Registerkarte "Konfigurieren", und klicken Sie dann auf "Benutzerspeicher".
3. Wählen Sie "Benutzerspeicher" aus dem Auswahlmenü "Benutzerspeicher" aus.
4. Für "Globale Benutzer/Globale Gruppen" wählen Sie "Verweis von einem externen LDAP-Verzeichnis" aus.

5. Wählen Sie "Mehrfache Microsoft Active Directory-Domänen" aus der Drop-down-Liste "Konfigurationstyp" aus.
6. Klicken Sie auf "Verzeichnis hinzufügen", und geben Sie den ersten Active Directory-Namen in das Feld "Name" ein.
7. Geben Sie unter "Domäneneinstellungen" die Domäne in das Feld "Domäne" ein.
8. Geben Sie den Hostnamen und die Portnummer in die Felder "Host" und Port ein, und klicken Sie dann auf den rechten Pfeil.

   Die Liste "Ausgewählte Hostnamen" gibt an, wo sich das Active Directory befindet.
9. Wählen Sie aus der Drop-down-Liste "Protokoll" das Protokoll aus, das Sie benötigen.
10. Geben Sie für "Basis-DN" (Base Distinguished Name) einen Wert ohne Leerzeichen ein. Der Wert gibt das externe LDAP-Verzeichnis an, das Daten für globale Anwender und globale Gruppen enthält. Im folgenden Beispiel schränkt der Wert "OU=" die geladenen globalen Gruppen auf die Gruppen in der angegebenen Organisationseinheit ein.

    ```
    OU=myorganizationalunit,DC=foo,DC=com
    ```
11. Geben Sie die Anmeldeinformationen an, die CA EEM verwenden soll, um auf die angegebene Domäne und Organisationseinheit zuzugreifen. Dieser Anwender muss ein Mitglied der Domäne und der Organisationseinheit sein, die für "Basis-DN" angegeben wurde.

    a. Geben Sie für "Anwender-DN" (User Distinguished Name) den allgemeinen Namen des Anwenders ein, der eine Verbindung mit dem externen LDAP-Verzeichnis herstellen soll. Verwenden Sie das Escape-Zeichen (\) vor einem Komma zwischen den Teilen des allgemeinen Namens. Zum Beispiel

       ```
       CN=Vorname\,Nachname,DC=foo,DC=com
       ```

    b. Geben Sie das Kennwort ein, das dem allgemeinen Namen zugeordnet ist, der für "Anwender-DN" für "Anwenderkennwort" und für "Kennwort bestätigen" angegeben ist.
12. Schließen Sie die erweiterte Konfiguration ab, oder akzeptieren Sie die Standardwerte.
13. Wiederholen Sie die Schritte 6 bis 12 für jedes AD, das referenziert werden soll.
14. Klicken Sie auf "Speichern".

    Wenn Sie die Konfiguration speichern, werden folgende Statusmeldungen angezeigt:

    - Externe Verzeichnisbindung erfolgreich.
    - Externe Verzeichnisdaten geladen.

Voraussetzungen für die Port-Planung

Ports werden während Installation konfiguriert. Wenn Sie Netzwerkports konfigurieren, akzeptieren Sie Standardwerte, außer wenn:

- Der Standardport wird von einer anderen Anwendung auf dem Host verwendet.
- Eine Firewall-Beschränkung verhindert die Kommunikation auf dem Standardport.

Überprüfen Sie die Verwendung der Ports in Von CA Process Automation verwendete Ports (siehe Seite 231), und planen Sie Ersetzungen für Ports, die in Ihrem Netzwerk oder auf dem entsprechenden Host verwendet werden. Mit Ausnahme des Ports für Agenten und für CA EEM werden alle anderen Eigenschaften in der Datei "OasisConfig.properties" unter "*install_dir*/server/c2o/.config" gespeichert. Wenn nach der Installation ein Konflikt auftritt, können Sie diese Datei manuell ändern.

Interaktive Installation des Domänen-Koordinationsrechners

Die Installation des CA Process Automation-Domänen-Koordinationsrechners hängt davon ab, ob bestimmte Komponenten vorhanden sind. Deswegen wird die Installation von CA Process Automation in zwei größeren Phasen durchgeführt:

1. Installieren der Drittanbieter-Software.
2. Installieren des Domänen-Koordinationsrechners.

Beide Schritte müssen ausgeführt werden, wenn Sie CA ProcessAutomation installieren, neu installieren oder ein Upgrade durchführen.

Die Installation kann über einen physischen Datenträger oder über eine Kopie des physischen Datenträger ausgeführt werden, oder sie können heruntergeladen werden.

Sie können den Installationsprozess jederzeit beenden. Wenn Sie die Installation abbrechen, wird ein Bestätigungsfenster eingeblendet. Wenn Sie den Abbruch bestätigen, werden die von Ihnen durchgeführten Installationsschritte rückgängig gemacht.

Wenn Sie einen Lastenausgleich haben, empfehlen wir, dass Sie den Domänen-Koordinationsrechner als geclustertern Koordinationsrechner einrichten, auch wenn Sie gegenwärtig keine Cluster planen. Wenn Sie zu einem späteren Zeitpunkt Clustern wollen und den Domänen-Koordinationsrechner nicht geclustert eingerichtet haben, müssen Sie den Domänen-Koordinationsrechner neu installieren, um Clustering zu unterstützen. Details finden Sie unter:

- Voraussetzungen des NGINX-Lastenausgleichs (siehe Seite 36).
- Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54).
- Voraussetzungen des Apache-Lastenausgleichs (siehe Seite 267).

Für nachfolgende Installationen sind bestimmte Werte erforderlich, die Sie während der Installation des Domänen-Koordinationsrechners konfigurieren. Zum Beispiel müssen während eines Upgrades oder einer Installation bestimmte Kennwörter oder andere Koordinationsrechner erneut eingegeben werden. Eine einfache Methode, um einen Datensatz mit den von Ihnen angegebenen Werten beizubehalten, ist, einen Plan für Kennwörter zu erstellen, bevor Sie mit der interaktiven Installation beginnen. Notieren Sie z. B. Kennwörter, die spezifisch für Datenbankserver sind, oder notieren Sie Kennwörter für Folgendes.

- CA Process Automation-Zertifikat.
- CA EEM-Zertifikat.
- Repository-Datenbank.
- Berichtsdatenbank.
- Laufzeitdatenbank.
- CA EEM-Administrator.

Weitere Informationen:

Unbeaufsichtigte Domänen-Koordinationsrechner-Installation (siehe Seite 121)

Installieren der Drittanbieter-Software

Sie beginnen die CA Process Automation-Installation mit der Installation der Software von Drittanbietern. Nach Abschluss dieser Installation beginnt die Installation des Koordinationsrechners automatisch.

Gehen Sie folgendermaßen vor:

1. Legen Sie DVD1 des CA Process Automation-Installationsdatenträgers in ein Laufwerk ein. Alternativ dazu können Sie Ihr System nach dem Speicherort der Ordner "DVD1" und "DVD2" durchsuchen, die Kopien der Installationsdateien enthalten.
2. Führen Sie das entsprechende Installationsprogramm auf Ihrer Plattform und Ihrem Datenträger aus:
   - **Windows:** Domain_Installer_windows.bat
   - **Linux oder UNIX:** Domain_Installer_unix.sh

   Diese Dateien rufen das Drittanbieter-Installationsprogramm und später das Installationsprogramm für den Domänen-Koordinationsrechner auf.

3. Wählen Sie die bevorzugte Sprache aus dem Dialogfeld zur Sprachauswahl aus.

   Dies legt die Standardsprache fest. Ungeachtet der ausgewählten Sprache wird CA Process Automation mit Support für alle verfügbaren Lokalisierungen installiert.

   Das Fenster "Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation" wird angezeigt.

4. Klicken Sie auf "Weiter", um die Installation der Drittanbieterkomponenten zu starten.

5. Lesen Sie die Lizenzvereinbarung. Wenn Sie die Bedingungen akzeptieren, wählen Sie "Ich akzeptiere die Bedingungen der Lizenzvereinbarung" aus, und klicken Sie auf "Weiter".

6. Klicken Sie auf "Weiter", um die Komponenten im Standardzielverzeichnis zu installieren. Oder wechseln Sie in ein anderes Verzeichnis, und klicken Sie dann auf "Weiter".

   Das Installationsprogramm erstellt den Ordner automatisch, wenn er nicht vorhanden ist. Es sind mindestens 8 GB Speicherplatz erforderlich.

   Wichtig! Stellen Sie sicher, dass die CA Process Automation-Ordnerstruktur einschließlich Installationsort nicht 255 Zeichen überschreitet. CA Technologies empfiehlt, für das Installationsverzeichnis (*Installationsverzeichnis*) höchsten 64 Zeichen zu verwenden.

   Die Liste von Drittanbietervoraussetzungen wird angezeigt. Die Drittanbietervoraussetzungen für den Domänen-Koordinationsrechner umfassen die Installation von JBoss, Hibernate und JDBC Jar. In CA Process Automation r 4.2 wird der ActiveMQ-Messaging-Service mit JBoss 5.1 verwendet.

7. Klicken Sie auf "Weiter", und überwachen Sie dann die Installation von JBoss und Drittanbieterkomponenten.

   Die JDBC Jar-Installation wird angezeigt.

8. Wählen Sie eine oder mehrere Anwendungen für den Datenbankserver aus, die für den internen Zugriff auf CA Process Automation-Datenbanken verwendet werden sollen, und geben Sie den Pfad zur entsprechenden JAR-Datei des JDBC-Treibers an. Klicken Sie anschließend auf "Weiter".

   - MySQL: Navigieren Sie zu einer JAR-Datei des JDBC-Treibers, die Sie vorher für MySQL heruntergeladen haben. Zum Beispiel:

     `...`*`your_dir`*`\mysql-connector-java-5.1.19-bin.jar`

   - MS SQL: Akzeptieren Sie den Standardpfad zur JTDS-JAR-Datei für JDBC auf dem Installationsdatenträger "DVD1". Zum Beispiel:

     `...\DVD1\drivers\jtds-1.3.jar`

     (Optional können Sie zu einer anderen JDBC Jar-Datei navigieren.)

   - Oracle: Akzeptieren Sie den Standardpfad zur JDBC Jar-Datei auf dem Installationsdatenträger "DVD1". Zum Beispiel:

     `...DVD1\drivers\ojdbc14.jar`

     (Optional können Sie zu einer anderen JDBC Jar-Datei navigieren.)

   Hinweis: Sie müssen mindestens einen JDBC-Treiber angeben. Das Angeben von mehreren JDBC-Treibern für die interne Kommunikation ist normalerweise nicht notwendig. Während der Installation des Domänen-Koordinationsrechners können Sie zusätzliche JDBC-Treiber für die Verwendung durch andere Koordinationsrechner oder Agenten mit den Datenbankoperatoren (dem früheren JDBC-Modul) installieren.

9. Wenn "Der Setup-Assistent für CA Process Automation wird ausgeführt" angezeigt wird, legen Sie die "DVD2" der CA Process Automation-Installation ein, oder ersetzen Sie im Feld "DVD1" durch "DVD2". (Alternativ können Sie in das Verzeichnis navigieren, das die Dateien vom DVD2-Installationsdatenträger enthält.) Klicken Sie dann auf "Fertig stellen".

   Das Installationsprogramm des Drittanbieters übergibt die Steuerung an das Installationsprogramm des CA Process Automation-Domänen-Koordinationsrechners. Möglicherweise kommt es zu einem kurzen Intervall, wenn die Anwenderoberfläche des Installationsprogramms des Drittanbieters geschlossen ist und die Anwenderoberfläche für die Installation der CA Process Automation-Domäne noch nicht angezeigt wird. Dies ist normal.

Installieren des Domänen-Koordinationsrechners

Nach der Installation von Drittanbieterkomponenten kopiert das Drittanbieter-Installationsprogramm die Dateien des CA Process Automation-Installationsprogramms auf den Host und startet das Installationsprogramm des Domänen-Koordinationsrechners.

Dieser Abschnitt beschreibt die Installation eines nicht geclusterten Domänen-Koordinationsrechners oder des ersten Knotens eines geclusterten Domänen-Koordinationsrechners.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Seite "Willkommen" auf "Weiter".
2. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".
3. Stellen Sie sicher, dass der angezeigte Pfad der Pfad zum Java-Home-Verzeichnis ist. Wenn der Pfad zum Java-Home-Verzeichnis nicht angezeigt wird, stellen Sie die folgenden Schritte fertig:
   a. Klicken Sie auf "Durchsuchen".
   b. Navigieren zum richtigen Speicherort
   c. Wählen Sie das zu verwendende Java Development Kit (JDK) aus. Wählen Sie z. B. Folgendes:

      ```
      C:\Program Files\Java\jdk1.7.0_21
      ```

   d. Klicken Sie auf "Weiter".

   Das JDK wird validiert.
4. Überwachen Sie den Fortschritt, während die Dateien kopiert werden.
5. Um CA Process Automation zur Verwendung mit CA SiteMinder zu konfigurieren, stellen Sie sicher, dass alle CA SiteMinder-Voraussetzungen erfüllt sind. Schließen Sie dann die folgenden Felder auf dem CA Process Automation-Domänenkonfigurationsbildschirm ab:

   Konfigurieren von Single Sign-on (SSO)

   Aktivieren Sie dieses Kontrollkästchen, um CA SiteMinder mit dem Domänen-Koordinationsrechner zu konfigurieren.

   Stellen Sie sicher, dass der CA SiteMinder-WebAgent mit dem gleichen Apache-Lastenausgleich konfiguriert wird, den Sie für CA Process Automation verwenden.

Authentifizierungstyp

Wählen Sie als Authentifizierungstyp **Header** aus, wenn CA SiteMinder konfiguriert ist.

Der Authentifizierungstyp entscheidet, wie CA Process Automation über die Anwender-ID informiert wird, wenn sich ein Anwender über CA SiteMinder angemeldet hat. Anwender können die in der Liste "SSO-Authentifizierungstyp" aufgefüllten Standardwerte auswählen.

SSO-Authentifizierungsparameter

Gibt den Namen des Authentifizierungsparameters an, wenn CA SiteMinder konfiguriert wird.

Akzeptieren Sie die Standardwerte, oder geben Sie neue Werte je nach Ihrer CA SiteMinder-Konfiguration ein.

- Wählen Sie **sm_user** als SSO-Authentifizierungsparameter für IIS aus.
- Wählen Sie **SM_User** als SSO-Authentifizierungsparameter für Apache aus.

Typ des Servers

Gibt die Installationsart als neuen Koordinationsrechner an.

6. Führen Sie die entsprechende Aktion aus:

   - Wenn Sie planen, einen geclusterten Domänen-Koordinationsrechner zu konfigurieren, lesen Sie die Anweisungen, und stellen Sie dann diesen Konfigurationsbildschirm fertig.
   - Wenn Sie den Domänen-Koordinationsrechner für die Verwendung mit CA SiteMinder konfigurieren, lesen Sie die Anweisungen, und stellen Sie dann diesen Konfigurationsbildschirm fertig.

   Lastenausgleich konfigurieren

   Gibt an, ob der Domänen-Koordinationsrechner mit der Möglichkeit zum Clustering installiert werden soll.

   Ausgewählt

   Installieren des Domänen-Koordinationsrechners mit der Möglichkeit zum Clustering. Bevor Sie diese Option aktivieren, stellen Sie sicher, dass die Voraussetzungen des NGINX-Lastenausgleichs (siehe Seite 35) bzw. die Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54) erfüllt sind.

   Gelöscht

   Installieren des Domänen-Koordinationsrechners ohne Möglichkeit zum Clustering.

   Worker-Knoten für den Lastenausgleich

   Definiert den Namen des Worker-Knotens für den Lastenausgleich. Da die erste Installation des Domänen-Koordinationsrechners der erste Knoten im Cluster ist, ist dieser Wert normalerweise "node1".

   Wenn Apache Ihr Lastenausgleich ist, muss Ihre Eingabe mit dem Knotennamen in der zugeordneten Variable "worker.*nodename.host*" mit diesem Host in der Apache-Datei "*Apache-Installationsverzeichnis*\conf\workers.properties" übereinstimmen. Im folgenden Beispiel ist der Variablenwert "**node1**" der Wert, der hier zugewiesen werden soll.

   `worker.`**`node1`**`.host=`*`DomainOrchestratorHostName`*

   Wenn in der Datei "workers.properties" der Wert "worker.**abc**.host" angegeben wäre, dann würden Sie "**abc**" eingeben.

   Wenn F5 Ihr Lastenausgleich ist, dann akzeptieren Sie den Standardwert. (Der Wert der Worker-Knoten ist für F5 nicht relevant, sodass kein Rückbezug zu den von Ihnen ausgeführten F5-Voraussetzungen vorhanden ist.)

   Standard: "node1" (Sonderzeichen, einschließlich Bindestriche, werden nicht unterstützt.)

Öffentlicher Hostname

Gibt den öffentlichen Hostnamen für den Apache-Server, NGINX-Server bzw. F5-Server an. Zum Beispiel:

`loadbalancerhost.mycompany.com`

- Legen Sie dieses Feld auf den FQDN von IIS/Apache fest, wo CA SiteMinder WebAgent konfiguriert wird, wenn Sie das Kontrollkästchen "Konfigurieren von Single Sign-on (SSO)" aktiviert haben.
- Legen Sie dieses Feld auf den FQDN des Apache-, F5- oder NGINX-Lastenausgleichs fest, wenn Sie das Kontrollkästchen "Lastenausgleich konfigurieren" ohne die Option "Konfigurieren von Single Sign-on (SSO)" aktiviert haben.

Portnummer des öffentlichen Hosts

Definiert den HTTP-Port für IIS/Apache (der öffentliche Host) oder für den F5-Host, wenn das Kontrollkästchen "Sichere Kommunikation unterstützen" deaktiviert ist.

Wenn Sie diesen Wert während der Installation und Konfiguration des Apache-, F5- oder NGINX-Lastenausgleichs ändern, müssen Sie diesen Wert entsprechend aktualisieren. Dieser Port und der Wert "Öffentlicher Hostname" werden verwendet, um zu CA Process Automation zu navigieren. Zum Beispiel:

`http://public-host-name:80/itpam`

Standard: 80

Sicherer Port des öffentlichen Hosts

Definiert den HTTPS-Port für den angegebenen öffentlichen Host, wenn das Kontrollkästchen "Sichere Kommunikation unterstützen" aktiviert ist.

Dieser Port ist ein Teil der URL, die verwendet wird, um auf CA Process Automation-Webservices zuzugreifen. Dieser Port und der Wert "Öffentlicher Hostname" werden verwendet, um zu CA Process Automation zu navigieren. Zum Beispiel:

`https://public-host-name:443/itpam`

Standard: 443

Sichere Kommunikation unterstützen

Gibt an, ob der Lastenausgleich (F5, NGINX, oder Apache) HTTPS für sichere Kommunikation verwendet.

Ausgewählt

Zeigt an, dass IIS oder Apache (der öffentliche Host) HTTPS verwendet, um zu kommunizieren.

Hinweis: Wenn Sie die Schritte "Konfigurieren der sicheren Kommunikation" für Apache ausführen, wählen Sie diese Option aus.

Zeigt an, dass F5 HTTPS verwendet, um zu kommunizieren.

Gelöscht

Zeigt an, dass IIS oder Apache (der öffentliche Host) HTTP verwendet, um zu kommunizieren.

Zeigt an, dass F5 HTTP verwendet, um zu kommunizieren.

7. Klicken Sie auf "Weiter".
8. Geben Sie im Feld "Unternehmen" Ihren Unternehmensnamen ein, und klicken Sie dann auf "Weiter".

   CA Process Automation zeigt Ihre Eingabe als Wert "Dieses Produkt ist lizenziert für" an, wenn Sie auf "Hilfe" und dann auf "Info" klicken.
9. Geben Sie ein Zertifikatskennwort ein, geben Sie es erneut ein, und klicken Sie dann auf "Weiter".

   Zertifikatskennwort

   Definiert das Kennwort, das den Zugriff auf die Schlüssel steuert, die zum Verschlüsseln der Kennwörter und anderer kritischer Daten verwendet werden. Verwenden Sie dasselbe Kennwort, wenn Sie einen anderen Koordinationsrechner installieren oder wenn Sie einem Koordinationsrechner Cluster-Knoten hinzufügen. Das Zertifikatskennwort ist einer einzelnen CA Process Automation-Domäne eigen.

   Zertifikatskennwort bestätigen

   Stimmt mit Ihrer Eingabe in diesem Feld mit Ihrer Eingabe im Feld "Zertifikatskennwort" überein, um das Kennwort zu verifizieren.

   Wichtig! Bevor Sie auf der Seite "Zertifikatskennwort festlegen" auf "Weiter" klicken, notieren Sie das Zertifikatskennwort, und bewahren Sie es an einem sicheren Ort als spätere Referenz auf. Dasselbe Zertifikatskennwort ist erforderlich, wenn Sie ein Upgrade des Domänen-Koordinationsrechners und anderer Koordinationsrechner (einschließlich Cluster-Knoten) auf eine neue Version durchführen.

10. (Nur für Windows) Geben Sie die folgenden Startmenüeinstellungen an, und klicken Sie dann auf "Weiter".

    [Name des Startmenüordners]

    Definiert den Namen des CA Process Automation-Startmenüordners, wenn Sie das Kontrollkästchen "Keinen Startmenüordner erstellen" deaktiviert haben. Akzeptieren Sie den Standard, oder geben Sie den Namen des Startmenüordners für CA Process Automation ein.

    Standard: CA Process Automation 4.0

    Erstellen von Verknüpfungen für alle Anwender

    Gibt an, ob die angegebene Verknüpfung des Menüordnernamens für alle Anwender angezeigt wird, die sich mit dem CA Process Automation-Domänen-Koordinationsrechner auf dem Server anmelden.

    Ausgewählt: Verknüpfungen werden angezeigt.

    Deaktiviert: Verknüpfungen werden nicht angezeigt.

    Keinen Startmenüordner erstellen

    Gibt an, ob im Startmenü eine Eingabe für CA Process Automation erstellt werden soll.

    Ausgewählt: Erstellen Sie einen Startmenü-Eintrag für CA Process Automation.

    Deaktiviert: Erstellen Sie keinen Startmenü-Eintrag für CA Process Automation.

11. Schließen Sie die folgenden Felder ab, um zu bestimmen, wie der Domänen-Koordinationsrechner mit anderen CA Process Automation-Komponenten und -Anwendungen kommuniziert, und klicken Sie dann auf "Weiter".

    Serverhost

    Definiert eine der folgenden Eigenschaften:

    - Der Hostname oder die IP-Adresse des Hostsystems, auf dem der Domänen-Koordinationsrechner bereitgestellt wird.
    - Ein DNS-Alias, der für den Host aufgelöst wird.

    Anzeigename

    Gibt den Namen des Domänen-Koordinationsrechners an, der im CA Process Automation-Konfigurationsbrowser angezeigt wird.

    - Wenn Sie keinen Lastenausgleich konfigurieren, ist der Anzeigename mit dem Hostnamen des Servers identisch.
    - Wenn Sie einen Lastenausgleich konfigurieren, entspricht der Anzeigename dem FQDN des Servers, auf dem der Lastenausgleich installiert ist.

Sichere Kommunikation unterstützen

Gibt an, ob die Kommunikation mit CA Process Automation im Gegensatz zur standardmäßigen einfachen Kommunikation sicher ist. Dieser Wert steuert, ob der HTTP-Port oder der HTTPS-Port aktiviert wird.

Ausgewählt: Verwenden Sie das HTTPS-Protokoll für die Kommunikation.

Deaktiviert: Verwenden Sie nicht das HTTPS-Protokoll für die Kommunikation. Verwenden Sie stattdessen HTTP.

Serverport

Gibt den Port an, den der Domänen-Koordinationsrechner verwendet, um mit anderen Koordinationsrechnern und Agenten zu kommunizieren.

Standard: 80 (Basis: HTTP) oder 443 (Gesichert: HTTPS)

HTTP-Port

Definiert den HTTP-Port, der für den Webserver verwendet wird, wenn das Kontrollkästchen "Sichere Kommunikation unterstützen" deaktiviert ist.

Hinweis: Dieser Port ist Teil der URL, die verwendet wird, um auf CA Process Automation-Webservices und das CA Process Automation-Anmeldefenster zuzugreifen.

Standard: 8080

HTTPS-Port

Wenn Sie "Sichere Kommunikation unterstützen" auswählen, bestimmt dieses Feld den in der URL verwendeten Port, der auf CA Process Automation-Webservices und die browserbasierte CA Process Automation-Benutzeroberfläche zugreift.

Standard: 8443

Hinweis: Sie müssen "Sichere Kommunikation unterstützen" aktivieren, um die Eingabe in dieses Feld zu ermöglichen.

JNDI-Port

Definiert den vom Webserver verwendeten Java-Naming-Server-Port.

Hinweis: Auf diesen Port darf nicht von außerhalb dieses Hostsystems zugegriffen werden.

Standard: 1099

RMI-Port

Definiert den RMI-Port, den der Webserver verwendet.

Hinweis: Auf diesen Port darf nicht von außerhalb dieses Hostsystems zugegriffen werden.

Standard: 1098

SNMP-Port

Definiert den SNMP-Trap-Listener-Port für CA Process Automation.

Standard: 162

12. Akzeptieren Sie den Standardpfad, oder navigieren Sie in ein temporäres Verzeichnis, in dem Skripte ausgeführt werden sollen. Klicken Sie auf "Weiter".

    Dieses Verzeichnis muss für alle Anwender beschreibbar sein.

13. Schließen Sie die folgenden Felder ab, um PowerShell-Einstellungen zu definieren, und klicken Sie dann auf "Weiter".

    PowerShell-Ausführungsrichtlinie festlegen

    Gibt an, ob die Verwendung von PowerShell aktiviert werden soll.

    Ausgewählt: Aktivieren Sie die Verwendung der PowerShell, die die PowerShell-Ausführungsrichtlinie am angegebenen Pfad auf "RemoteSigned" (per Remote-Zugriff signiert) festlegt.

    Deaktiviert: Deaktivieren Sie die Verwendung der PowerShell.

    PowerShell-Pfad auf Hostrechner

    CA Process Automation erkennt den PowerShell-Pfad automatisch.

    Hinweis: Wenn Sie auf "Weiter" klicken, validiert das Installationsprogramm den angegebenen PowerShell-Pfad.

14. Geben Sie die CA EEM-Sicherheitseinstellungen an. Die Reihenfolge, in der Felder in diesem Schritt angezeigt werden, basiert auf den Abhängigkeiten statt auf der Feldreihenfolge, die auf der Benutzeroberfläche angezeigt wird.

    a. Füllen Sie folgende erforderliche Felder aus:

    EEM Server

    Definiert den FQDN des CA EEM-Servers, den CA Process Automation verwendet, um CA Process Automation-Anwender zu authentifizieren und zu autorisieren. Wenn Sie EEM für die Hochverfügbarkeit konfigurieren, können Sie auch einen Sicherungs-CA EEM-Server definieren. Verwenden Sie ein Komma als Trennzeichen zwischen den Servernamen.

    EEM-Anwendungsname

    Definiert, wie der CA Process Automation-Anwendungsname in CA EEM angezeigt wird. Wenn Sie gleichen CA EEM-Server mit mehreren Domänen von CA Process Automation verwenden, muss jede CA Process Automation-Domäne einen eindeutigen EEM-Anwendungsnamen erhalten. Der Name, den Sie hier eingeben, wird in der Drop-down-Liste der Anmeldungsseite des CA EEM-Servers angezeigt.

    Wenn Sie ein Upgrade durchführen, ist dieses Feld bereits mit dem Wert aufgefüllt, der in der Erstinstallation verwendet wurde. Dieser Wert behält die Zuordnungen der CA EEM-Anwendergruppen, anwenderdefinierte Richtlinien und anwenderspezifische Gruppen bei. CA EEM verwendet diesen Wert, um diese CA Process Automation-Domäne zu identifizieren.

    Standard: Process Automation

    FIPS-konformes Zertifikat verwenden

    Gibt an, ob FIPS-konforme Zertifikate verwendet werden sollen. Diese Einstellung muss mit der CA EEM-Einstellung für FIPS-Modus übereinstimmen.

    Hinweis: Um die CA EEM-Einstellung für FIPS zu bestimmen, klicken Sie in CA EEM auf "Info". Die Produktspezifikationen enthalten "FIPS-deaktiviert" oder "FIPS-aktiviert".

    Aktiviert: FIPS-Modus ist in CA EEM eingeschaltet.

    Deaktiviert: FIPS-Modus ist in CA EEM ausgeschaltet.

b. Geben Sie Ihre *Absicht zur Registrierung* des angegebenen Anwendungsnamens für diese CA Process Automation-Domäne mit CA EEM an, nachdem Sie diese Seite ausgefüllt haben. Der Registrierungsprozess generiert basierend auf Ihrer Auswahl entweder FIPS-kompatible Zertifikate oder nicht-FIPS-kompatible Zertifikate. Dieses Kontrollkästchen wird über der Schaltfläche "Registrieren" angezeigt. "Auswahl" ist die typische Konfiguration.

Anwendung mit CA EEM registrieren

Gibt an, ob der Wert "EEM-Anwendungsname" für CA Process Automation mit CA EEM registriert und das Zertifikat generiert werden soll, das CA Process Automation verwendet, um eine Verbindung mit der Anwendung auf dem CA EEM-Server herzustellen. Das CA EEM-SDK verarbeitet die Verbindung. Wenn Sie dazu aufgefordert werden, geben Sie an, dass Sie ein Upgrade der CA Process Automation-Anwendung in CA EEM durchführen möchten.

Ausgewählt: Die Schaltfläche "Registrieren" wird ausgewählt. (Siehe Schritt 16.) Deaktiviert das Feld "EEM-Zertifikatsdatei". Bei einer neuen Installation eines Domänen-Koordinationsrechners müssen Sie dieses Kontrollkästchen immer auswählen. Wenn Sie die Felder unter "EEM-Sicherheitseinstellungen" ausgefüllt haben, klicken Sie auf "Registrieren".

Deaktiviert: Die Auswahl der Schaltfläche "Registrieren" wird aufgehoben. Aktiviert das Feld "EEM-Zertifikatsdatei".

c. Füllen Sie bei einer neuen Installation das folgende Feld nur dann aus, wenn Sie die Anwendung nicht mit CA EEM registrieren. Klicken Sie auf "Durchsuchen", und navigieren Sie zum Speicherort der Zertifikatsdatei. Sobald die Zertifikatsdatei hochgeladen ist, fügt das Installationsprogramm die Datei in dieses Verzeichnis ein:

`Installationsverzeichnis/server/c2o/.c2orepository/public/certification`

Hinweis: Wenn Sie ein Upgrade durchführen, wird dieses Feld automatisch mit dem Pfad zu Ihrer Zertifikatsdatei aufgefüllt.

EEM-Zertifikatsdatei

Definiert die für CA Process Automation zu verwendende CA EEM-Zertifikatsdatei. Normalerweise können Sie den Standardwert akzeptieren.

Standardeinstellungen:

"PAM.cer", wenn Sie das Kontrollkästchen "FIPS-konformes Zertifikat verwenden" aktiviert haben.

"PAM.p12", wenn Sie das Kontrollkästchen "FIPS-konformes Zertifikat verwenden" deaktiviert haben.

d. Füllen Sie bei Bedarf eines der folgenden Felder aus.

Zertifikats-Schlüsseldatei

Klicken Sie bei Bedarf (siehe "Hinweise") auf "Durchsuchen", und navigieren Sie zum Speicherort des Zertifikatsschlüssels, zum Beispiel die Datei "PAM.key". Sobald die Zertifikatsdatei hochgeladen ist, fügt das Installationsprogramm die Datei in dieses Verzeichnis ein:

Installationsverzeichnis`/server/c2o/.c2orepository/public/certification`

Hinweise:

- Wenn es sich um eine neue Installation handelt, ist dieses Feld nicht erforderlich, wenn Sie FIPS verwenden und beabsichtigen, sich anzumelden. (Der Registrierungsprozess generiert die Zertifikatsschlüsseldatei mit dem Zertifikat.)
- Wenn es sich um eine neue Installation handelt, ist dieses Feld erforderlich, wenn Sie FIPS verwenden und nicht beabsichtigen, sich anzumelden.
- Wenn Sie ein Upgrade durchführen, wird dieses Feld mit dem Pfad zu Ihrer Schlüsseldatei aufgefüllt.

EEM-Zertifikatskennwort

Erforderlich, wenn Sie FIPS nicht verwenden. Definiert das CA EEM-Zertifikatskennwort. Dieses Kennwort schützt das Zertifikat "PAM.p12". CA Process Automation benötigt dieses Kennwort, um das Zertifikat "PAM.p12" zu öffnen und zu verwenden.

e. Füllen Sie folgende Felder nur dann aus, wenn Sie CA EEM konfigurieren, um auf Anwender von einem externen LDAP-Verzeichnis zu verweisen. Anderenfalls überspringen Sie diesen Schritt.

Standardmäßige Active Directory-Domäne

(Nur anwendbar, wenn Sie planen, bei der Konfiguration der Version 12.51 von CA EEM auf mehrere Active Directory-Domänen zu verweisen. Weitere Informationen finden Sie unter Schritt 17.) Gibt die AD-Domäne an, die als Standarddomäne verwendet werden soll. CA Process Automation-Anwender, die zur hier angegebenen Domäne gehören, können sich mit ihrem nicht vollständigen Anwendernamen bei CA Process Automation anmelden. Anwender, die zu anderen AD-Domänen gehören, müssen ihren Prinzipalnamen (*domain**username* oder *username*@*domain*) und ihr Kennwort angeben, wenn sie sich bei CA Process Automation anmelden. Diese Eingabe muss mit der Eingabe im Feld "Domäne" für eine der mehreren AD-Domänen übereinstimmen, die Sie für den CA EEM-referenzierten Anwenderspeicher konfigurieren.

CA EEM muss entsprechend konfiguriert sein, um das "username@domain"-Formular des Prinzipalnamens zu authentifizieren.

Hinweis: Weitere Informationen finden Sie unter Konfigurieren von CA EEM, um es referenzierten Anwendern zu ermöglichen, sich mit ihrem E-Mail-Namen anzumelden (siehe Seite 136).

NTLM-Durchleitungs-Authentifizierung aktivieren

Gibt an, ob CA EEM das NTLM-Protokoll verwendet, um CA Process Automation-Anwender zu authentifizieren.

Ausgewählt: Aktiviert die NTLM-Durchleitungs-Authentifizierung. CA EEM verwendet das NTLM-Protokoll, um Anwender zu authentifizieren, die zu CA Process Automation navigieren.

Deaktiviert: Deaktiviert NTLM-Durchleitungs-Authentifizierung. Anwender, die zu CA Process Automation navigieren, müssen Anmeldeinformationen in das CA Process Automation-Anmeldedialogfeld eingeben. CA EEM validiert die Anmeldeinformationen mit den referenzierten Microsoft Active Directorys, um Anwender zu authentifizieren.

15. Registrieren Sie entweder den konfigurierten Wert "EEM-Anwendungsname" mit CA EEM oder überspringen Sie die Registrierung. Der Registrierungsprozess generiert CA Process Automation-Zertifikate der erforderlichen Länge.

    - Wenn dies eine neue Installation ist, klicken Sie auf "Registrieren", füllen Sie folgende Felder im Fenster "EEM-Anmeldeinformationen" aus, und klicken Sie auf "OK". Wenn die Bestätigung "Anwendung registriert" angezeigt wird, klicken Sie auf "OK".

      EEM-Admin-Anwendername

      Definiert den Anwendernamen des CA EEM-Administrators. Geben Sie **EiamAdmin** ein.

      EEM-Admin-Kennwort

      Gibt das Kennwort für das Anwenderkonto "EiamAdmin" an. Wenn Sie CA EEM installiert haben, geben Sie das Kennwort ein, das Sie für den EiamAdmin-Anwender erstellt haben. Setzen Sie sich ansonsten mit dem CA EEM-Administrator in Verbindung, um das Kennwort zu erhalten.

    - Wenn FIPS-Zertifikate verwendet werden, überschreiben die neuen Zertifikate "PAM.cer" und "PAM.key" die vorhandenen Zertifikate, sofern vorhanden. Wenn keine FIPS-Zertifikate verwenden, dann überschreibt das neue PAM.p12-Zertifikat das vorhandene Zertifikat in CA Process Automation, sofern vorhanden. Dieses Zertifikat ist durch das Kennwort geschützt, das Sie in das Feld "EEM-Zertifikatskennwort" eingegeben haben. Die EEM-Zertifikatsdatei wird mit einem Pfad und mit einem Dateinamen aufgefüllt, ähnlich wie in diesem Beispiel:

      `Installationsverzeichnis/server/c2o/.c2orepository/public/certification/PAM.p12`

      Hinweis: Die Zertifikate werden nicht neu generiert, wenn Sie zum Upgrade der CA Process Automation-Anwendung CA Embedded Entitlements Manager aufgefordert werden und Sie das Upgrade *nicht* durchführen.

Folgende Aufzählungsliste beschreibt die Anwendungsfälle:

- Neue Installation mit Registrierung: Der Installationsprozess entdeckt die CA EEM-Serverversion und wählt das entsprechende SDK aus.
- Neue Installation ohne Registrierung: Beim Installationsprozess werden Sie dazu aufgefordert, basierend auf der CA EEM-Release-Version ein SDK auszuwählen. Wenn Sie die Release-Version des CA EEM-Servers nicht kennen, melden Sie sich bei CA EEM an, und überprüfen Sie "Info".

Wählen Sie die Hauptversion von EEM SDK aus.
Wählen Sie EEM SDK 8, um eine Verbindung zu einem EEM 8.4-Server herzustellen
Wählen Sie EEM SDK 12, um eine Verbindung zu anderen unterstützten EEM-Servern herzustell...
Wählen Sie die Hauptversion von EEM SDK.
8
OK

16. (Optional) Wenn Sie die CA EEM-Einstellungen testen möchten und CA EEM so konfiguriert haben, dass Verweise von einem externen Verzeichnis verwendet werden, müssen Sie zunächst einen Testanwender erstellen. Ein Testanwender ist ein Anwender, den Sie aus einem ausgewählten Active Directory-Verzeichnis abrufen und zur PAMAdmins-Gruppe zuweisen. Gehen Sie folgendermaßen vor:

    a. Durchsuchen Sie das System nach der CA EEM-Instanz, die von CA Process Automation verwendet wird. Verwenden Sie folgende URL:

       `https://Hostname:5250/spin/eiam`

       Das Dialogfeld "CA Embedded Entitlements Manager" wird geöffnet.

    b. Wählen Sie in der Drop-down-Liste "Anwendung" den Namen aus, den Sie im Feld "EEM-Anwendungsname" konfiguriert haben.

    c. Tippen Sie "EiamAdmin" und das CA EEM-Administratorkennwort, das Sie konfiguriert haben.

    d. Klicken Sie auf Anmelden.

    e. Klicken Sie auf die Registerkarte Identitäten verwalten.

    f. Wählen Sie unter Benutzer suchen, wo "Globale Benutzer" aktiviert ist, Nachname oder "Vorname" aus, und geben Sie Ihren Vornamen bzw. Nachnamen in das Feld Wert ein. Klicken Sie anschließend auf Los. (Teilwerte werden akzeptiert.)

       Ihr Name wird unter "Anwender" im Bereich "Anwender" angezeigt.

    g. Doppelklicken Sie auf Ihren Namen, um Ihr geladenes Anwenderkonto anzuzeigen.

       Ihr Anwenderkonto hat zwei "Benutzerdetails"-Bereiche. Der obere Abschnitt lässt Sie eine Gruppe für Ihre Rolle in CA Process Automation definieren. Der untere Abschnitt: "Globaler Benutzer – Details" enthält Information vom externen Verzeichnis.

    h. Klicken Sie unter dem obersten Abschnitt auf die Schaltfläche Anwendungsbenutzerdetails hinzufügen.

       Die Liste "Verfügbare Benutzergruppen" enthält eine Gruppe für jede Standardrolle.

    i. Wählen Sie PAMAdmins aus, und klicken Sie auf den rechtsgerichteten Pfeil, um diese Gruppe in die Liste "Ausgewählte Benutzergruppen" zu verschieben.

    j. Klicken Sie auf "Speichern".

    k. Klicken Sie auf "Abmelden".

17. (Optional) Testen Sie die CA EEM-Einstellungen. Dieser Schritt erfordert, dass Sie die Anmeldeinformationen eines in CA EEM definierten Anwenders eingeben. Wenn Sie CA EEM als lokales Verzeichnis verwenden (Standard), können Sie die Anmeldeinformationen eines Standardanwenders eingeben. Wenn CA EEM auf ein externes Verzeichnis verweist, geben Sie Ihre eigenen Anmeldeinformationen ein (nachdem Sie den vorigen Schritt ausgeführt haben).

    a. Klicken Sie auf "CA EEM-Einstellungen testen".

    b. Wenn Sie CA EEM als lokales Verzeichnis verwenden und dies eine Neuinstallation ist, geben Sie "pamadmin" als Anwendernamen und als Kennwort ein, und klicken Sie auf "OK".

    c. Wenn Sie ein referenziertes Anwenderkonto von einem externen Verzeichnis verwenden, geben Sie die Anmeldeinformationen des Anwenders ein, wie dies im externen Verzeichnis definiert ist. Dies ist das Konto des Testanwenders, den Sie im vorigen Schritt erstellt haben.

    Auf dem Bildschirm "EEM-Einstellungen überprüfen" werden folgende Felder angezeigt:

    Verbinden

    Zeigt an, ob eine Verbindung zum angegebenen CA EEM-Server mit den in den CA EEM-Einstellungen bereitgestellten Werten hergestellt werden kann.

    Beschränkungen: "OK" und "NICHT OK"

    Hinweis: Wenn sich der Wert als "NICHT OK" erweist, werden die folgenden Felder nicht angezeigt.

    Der angegebene Anwender gehört zur Anwendergruppe.

    Zeigt an, ob der Anwender authentifiziert werden kann, d. h., ob die Anmeldung zulässig ist.

    Beschränkungen: "OK" und "NICHT OK"

    Der Anwender ist ein Admin.

    Zeigt an, ob der Anwender autorisiert ist, Administratorenaufgaben auszuführen. Mitglieder der Gruppe "PAMAdmins" verfügen über diese Autorisierung.

    Beschränkungen: "Ja" und "Nein"

    EEM-Upgrade

    Zeigt an, ob für das CA Process Automation-Anwendungsschema im EEM-Server ein Upgrade durchgeführt wird. Wenn die Meldung "Es ist kein Upgrade erforderlich" angezeigt wird, klicken Sie auf "OK".

    Hinweis: Dieses Feld wird nur angezeigt, wenn der Wert NICHT OK ist. Wenn der Wert "NICHT OK" ist, führen Sie ein Upgrade für die Instanz durch.

18. Nachdem Sie die Ergebnisse überprüft haben, klicken Sie auf "OK" und dann auf "Weiter".

19. Schließen Sie die folgenden Felder ab, um die Bibliotheksdatenbankeinstellungen zu definieren (d. h. die Repository-Datenbank).

    Typ der Datenbank

    Gibt den Typ des Datenbanksystems an. Wählen Sie einen unterstützten Typen in der Drop-down-Liste aus.

    Werte: MySQL, MS SQL, Oracle

    Hinweis: Wir empfehlen, dass Sie entweder MS SQL oder Oracle auswählen, wenn diese Installation zur Produktionsverwendung bestimmt ist. MySQL ist eine geeignete Wahl für einen wenig ausgelasteten Domänen-Koordinationsrechner.

    Anwendername

    Gibt den Namen eines Anwenders an, der dazu autorisiert ist, die Datenbank auf dem Datenbankserver zu erstellen bzw. darauf zuzugreifen. Das Konto muss über die Berechtigungen verfügen, um die Datenbank auf dem Server zu erstellen oder Besitzer (DBO) einer vorhandenen Datenbank sein zu können. Die folgenden Werte werden basierend auf der Datenbankauswahl automatisch aufgefüllt:

    - MS SQL: **sa**
    - MySQL: **root**

    Kennwort

    Definiert das Kennwort, das mit dem angegebenen Anwendernamen verbunden ist.

    Datenbankserver

    Definiert den Hostnamen oder die IP-Adresse des Datenbankservers.

    - Wenn Sie "Typ der Datenbank" als "MS SQL" konfiguriert haben und Sie nur über eine SQL Server-Instanz auf dem Hostserver verfügen oder wenn Sie einen anderen Datenbanktyp ausgewählt haben, dann geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers an. (Dieser Name ist die Standardinstanz.)
    - Wenn Sie "Typ der Datenbank" als "MS SQL" konfiguriert haben und Sie über mehrere SQL Server-Instanzen auf dem Hostserver verfügen, dann geben Sie die Instanz mit dem Namen SQL Server an. Verwenden Sie das Format "Host\Instanz", zum Beispiel: *dbserver.mycompany*.com*pamdb.*
    - Wenn Sie "Typ der Datenbank" als "Oracle" konfiguriert haben, dann geben Sie einen SID-Namen an.

Datenbank-Port

Definiert den Verbindungsport, der auf dem Datenbankserver konfiguriert ist.

- Für MS SQL ist der Standardport 1433.
- Für MySQL ist der Standardport 3306.
- Für Oracle ist der Standardport 1521.

Repository-Datenbank

Definiert den Namen der Datenbank, in der Bibliotheksobjekte und andere Daten gespeichert werden sollen.

Jeder Koordinationsrechner kann über sein eigenes Repository, seine eigene Bibliothek oder Datenbank verfügen. Sie können die Bibliotheksdatenbank über Koordinationsrechner hinweg gemeinsam nutzen. Jede Datenbank muss einen eindeutigen Namen haben. Sie sollten mit dieser Erstinstallation die Einrichtung einer Namenskonvention für Ihre CA Process Automation-Datenbanken in Erwägung ziehen.

Treiber-JAR

Definiert die JAR-Datei des JDBC-Treibers für den angegebenen Datenbanktypen. Im Treiberordner im Ordner "DVD1" der Installationsmedien sind standardmäßige Treiber für Microsoft SQL Server Server und Oracle-Datenbankserver enthalten.

Standardeinstellungen:

SQL Server: jtds-1.3.jar

Oracle: ojdbc14.jar

MySQL: Klicken Sie auf "Durchsuchen", navigieren Sie zur heruntergeladenen JAR-Datei (beispielsweise "mysql-connector-java-5.1.18-bin.jar").

Datenbanksortierung

Definiert die Regeln für das Sortieren von Daten für MS SQL und Oracle. Sowohl die Groß- und Kleinschreibung als auch Akzentzeichen, Kana-Zeichentypen und Zeichenbreite können ein Teil des Regelsatzes sein. Dieses Feld ist eine Drop-down-Liste. Es empfiehlt sich, den Standardwert zu akzeptieren. Dieses Feld ist nicht auf MySQL anwendbar.

Standard: SQL_Latin1_General_CP1_CI_AS

Verbindungszeichenfolge verwenden

Aktivieren Sie dieses Kontrollkästchen, um Verbindungszeichenfolge anzugeben, um eine Verbindung zur Oracle-Datenbank herzustellen.

Hinweis: Dieses Kontrollkästchen ist nur für Oracle-Datenbanken aktiviert.

Verbindungszeichenfolge

Geben Sie eine JDBC-Verbindungszeichenfolge in einem der folgenden Formate ein:

`jdbc:oracle:thin:`*`DatabaseServer`*`:`*`PortNumber`*`:`*`DatabaseName`*

`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=`*`hostname`*`)(PORT=`*`portnumber`*`))`
`(CONNECT_DATA=(SERVICE_NAME=`*`serviceid`*`)))`

20. Klicken Sie auf "Datenbankeinstellungen testen", um die Konnektivität von CA Process Automation zum angegebenen Datenbankserver mithilfe des angegebenen Datenbankports und mit der angegebenen JAR-Datei zu testen.

    Wenn eine Meldung darauf hinweist, dass die Datenbanken fehlen, schließen Sie die Meldung, und klicken Sie auf "Datenbank erstellen". Außer Oracle können vom Koordinationsrechner benötigte Datenbanken während der Installation erstellt werden.

    Datenbank erstellen

    Erstellen Sie die Repository-Datenbank, wenn Sie MS SQL oder MySQL angegeben haben.

    Hinweis: Wenn ein Oracle-Datenbankserver verwendet wird, haben Sie bereits die Repository-Datenbank als Teil der Aufgaben für die Datenbankserver-Voraussetzungen erstellt.

    Eine Meldung zeigt an, dass eine Datenbank mit dem von Ihnen angegebenen Namen erstellt wurde. Klicken Sie auf OK. Klicken Sie wieder auf "Datenbankeinstellungen testen".

21. Klicken Sie auf "Weiter".

22. Geben Sie die Informationen der Laufzeitdatenbank ein, entweder manuell oder indem Sie Spezifikationen von Ihren Einträgen für die Repository-Datenbank kopieren. Klicken Sie auf "Datenbank erstellen" wenn "Typ der Datenbank" entweder MSSQL oder MySQL aufweist. Klicken Sie auf "Datenbankeinstellungen testen".

    Die Laufzeitdatenbank-Felder ähneln den Feldern für die Datenbankeinstellung für die Repository-Datenbank (Bibliotheksdatenbank), mit Ausnahme von zwei Feldern. Beschreibungen der weiteren Felder finden Sie unter Schritt 20.

    kopieren aus Haupt-Repository

    Gibt an, ob Einstellungen der Bibliotheksdatenbank in das Einstellungsfenster der Laufzeitdatenbank kopiert werden sollen.

    Ausgewählt: Kopiert die Einstellungen der Bibliotheksdatenbank in dieses Dialogfeld. Mit dieser Option können Sie Zeit sparen, wenn Sie den gleichen Datenserver für beide CA Process Automation-Datenbanken verwenden. Wenn Sie diese Option auswählen, geben Sie den Namen der Laufzeitdatenbank in das Feld "Laufzeitdatenbank" ein. Klicken Sie dann auf "Datenbankeinstellungen testen". Klicken Sie dann auf "Datenbank erstellen".

    Deaktiviert: Die Einstellungen der Bibliotheksdatenbank werden nicht in dieses Dialogfeld kopiert. Verwenden Sie diese Option, wenn Sie einen anderen Datenbanktyp für Laufzeitdaten als für Bibliotheksdatensätze verwenden.

    Laufzeitdatenbank

    Gibt den Namen der Datenbank oder des Schemas an, in der bzw. dem Laufzeitinstanzen gespeichert werden. Zwei Koordinationsrechner können nicht gleichzeitig auf die gleiche Laufzeitdatenbank zeigen. Geben Sie einen eindeutigen Namen ein.

    Standard: pam

    Wichtig! Es ist nicht möglich, Laufzeitdatenbanken über Koordinationsrechner gemeinsam zu nutzen. Wenn Sie CA Process Automation deinstallieren und dann erneut installieren, ändert sich die hier von Ihnen konfigurierte Laufzeitdatenbank nicht.

23. Klicken Sie auf "Weiter".

24. Konfigurieren Sie die Berichtsdatenbank wie folgt:

    - Wenn Sie denselben Datenbankserver für die Berichtsdatenbank verwenden, den Sie für die Repository-Datenbank verwenden:

        a. Geben Sie einen eindeutigen Namen für die Berichtsdatenbank im Feld "Berichtsdatenbank" ein.

        b. Aktivieren Sie das Kontrollkästchen "kopieren aus Haupt-Repository", um freigegebene Daten automatisch einzugeben.

        c. Klicken Sie auf "Datenbankeinstellungen testen".

        d. Klicken Sie auf "Datenbank erstellen" wenn der Datenbanktyp MS SQL oder MySQL ist.

    - Wenn Sie einen anderen Datenbankserver für die Berichtsdatenbank verwenden, als Sie für die Repository-Datenbank verwenden:

        a. Geben Sie einen eindeutigen Namen für die Berichtsdatenbank im Feld "Berichtsdatenbank" ein.

        b. Deaktivieren Sie das Kontrollkästchen "kopieren aus Haupt-Repository".

        c. Wählen Sie den Datenbanktypen aus der Drop-down-Liste "Typ der Datenbank" aus.

        d. Geben Sie im Feld "Anwendername" einen Anwendernamen ein, der dazu autorisiert ist, die Datenbank auf dem Datenbankserver zu erstellen bzw. darauf zuzugreifen. (Geben Sie zum Beispiel "sa" für MS SQL ein oder "root" für MySQL.)

        e. Klicken Sie auf "Datenbankeinstellungen testen".

        f. Klicken Sie auf "Datenbank erstellen" wenn der Datenbanktyp MS SQL oder MySQL ist. (Klicken Sie nicht auf diese Schaltfläche, wenn die Berichtsdatenbank auf einem Oracle-Datenbankserver ausgeführt wird.)

    Siehe folgende Feldbeschreibungen:

    kopieren aus Haupt-Repository

    Gibt an, ob Einstellungen der Bibliotheksdatenbank in das Einstellungsfenster der Berichtsdatenbank kopiert werden soll. Die Berichtsdatenbank-Felder ähneln den Feldern für die Datenbankeinstellung für die Repository-Datenbank (Bibliotheksdatenbank), mit Ausnahme von zwei Feldern. Beschreibungen der weiteren Felder finden Sie unter Schritt 20.

    Ausgewählt: Kopiert die Einstellungen der Repository-Datenbank in dieses Dialogfeld. Mit dieser Option können Sie Zeit sparen, wenn Sie den gleichen Datenserver für beide CA Process Automation-Datenbanken verwenden.

    Deaktiviert: Die Einstellungen der Repository-Datenbank werden nicht in dieses Dialogfeld kopiert. Verwenden Sie diese Option, wenn Sie einen anderen Datenbanktyp für Berichtsdaten als für Laufzeitdatensätze verwenden.

    Berichtsdatenbank

Gibt den Namen der Berichtsdatenbank an, in der alle generierten Berichte gespeichert werden. Geben Sie einen eindeutigen Namen ein.

25. Klicken Sie auf "Weiter".

26. Wählen Sie die zusätzlichen JAR-Dateien und typische JDBC-Treiber aus, die Sie in die Installation aufnehmen möchten.

    Standardmäßig werden die JDBC-Treiber, die während der Installation der Drittanbieter-Software hochgeladen wurden, angezeigt und sind nicht ausgewählt. Sie können die Schaltfläche "Dateien hinzufügen" verwenden, um weitere JAR-Dateien hinzuzufügen.

    Wählen Sie jede bereitzustellende JAR-Datei aus. Stellen Sie sicher, dass Sie alle Treiber ausgewählt haben, die Sie für die JDBC-Operator-Nutzung auf CA Process Automation-Agenten und -Koordinationsrechnern bereitstellen möchten. Sie können die Schaltfläche "Dateien hinzufügen" verwenden, um weitere Treiber hinzuzufügen.

    Es ist nicht notwendig, den Bedarf an Designern für JDBC-Treiber im Voraus miteinzubeziehen. Ein Domänenadministrator kann JDBC-Treiber bei Bedarf bereitstellen.

    Hinweis: Weitere Informationen über das Hinzufügen und Verwalten von Koordinationsrechnern und Agentenressourcen, einschließlich JDBC-JAR-Dateien, sind dem Handbuch für Inhaltsadministratoren zu entnehmen.

    Wenn Sie mit Ihrer Auswahl der JAR-Dateien zufrieden sind, klicken Sie auf "Weiter".

27. Überwachen Sie den Installationsfortschritt. Das Installationsprogramm kopiert und signiert alle CA Process Automation-Komponenten. Die Installation kann ein paar Minuten in Anspruch nehmen.

28. Klicken Sie auf "Fertig stellen", um die Installation zu beenden.

    Die Installation des Domänen-Koordinationsrechners ist abgeschlossen.

    Wenn Sie CA Process Automation nach einem Upgrade oder einer Installation zum ersten Mal starten, kann dies eine Weile dauern, da das Produkt das Datenbankschema einstellen muss. Rechnen Sie mit etwa einer Stunde pro GB an Daten. Die tatsächliche Dauer variiert allerdings je nach DBMS-Anbieter, Rechnerspezifikationen und Datenvolumen. Starten Sie den Koordinationsrechner (siehe Seite 143). Stellen Sie sicher, dass dieser erste Koordinationsrechner ordnungsgemäß funktioniert, bevor Sie mit der Installation bzw. dem Upgrade weiterer Systemkomponenten fortfahren.

Unbeaufsichtigte Domänen-Koordinationsrechner-Installation

CA Process Automation stellt die Option bereit, den Domänen-Koordinationsrechner mithilfe einer Antwortdatei automatisch oder unbeaufsichtigt zu installieren. Die Antwortdatei enthält verschiedene vordefinierte Parameter, die während des Installationsprozesses verwendet werden. Sobald Sie eine Antwortdatei erstellt haben, können Sie die Skriptdatei für die Installation bearbeiten und ausführen, um mit der Installation zu beginnen.

Eine Beispielantwortdatei befindet sich im Stammordner auf DVD1. Wir empfehlen Ihnen, eine Kopie dieser Datei als Basis für Ihre Antwortdatei zu verwenden.

Eine Antwortdatei erstellen

Der erste Schritt zur Ausführung einer automatischen Installation von CA Process Automation ist, eine Antwortdatei zu erstellen.

Berücksichtigen Sie die folgenden Hinweise in Bezug auf die Antwortdatei:

- Ändern Sie die Variablennamen nicht, da die Installation die vorhandenen Variablennamen verwendet.
- Verwenden Sie Schrägstriche (/) als Verzeichnistrennzeichen, um Speicherorte anzugeben.
- Verwenden Sie das Rautezeichen (#), um Variablen, die Sie nicht verwenden möchten, zu versehen.
- Siehe folgendes Installationsprotokoll, um Fehler zu überprüfen:

  ```
  ${install_dir}/server/c2o/installation.log
  ```

Gehen Sie folgendermaßen vor:

1. Legen Sie Disc 1 der CA Process Automation-Installationsdatenträger in ein Laufwerk ein, oder wechseln Sie zu dem Speicherort, an den die Installationsdateien zuvor von den Installationsdatenträgern kopiert wurden.
2. Öffnen Sie den Ordner "DVD1".

3. Öffnen Sie die folgende Datei.

   `response.varfile`

4. Geben Sie die entsprechenden Parameterwerte an.

   "varfile" enthält Parameterbeschreibungen. Verwenden Sie folgende Einstellung, damit CA EEM das NTLM-Protokoll verwenden kann, um CA Process Automation-Anwender zu authentifizieren:

   `enableNTLM=true`

   Die erforderlichen Parameter sind hier zu finden.

5. Speichern Sie "varfile" im Pfad, in dem die Skriptdatei für die automatische Installation enthalten ist.

   Die Antwortdatei wird erstellt.

Erforderliche Parameter in der Datei "response.varfile"

Wie bereits erwähnt, befindet sich im Stammordner auf DVD1 ein Beispiel einer Antwortdatei. Die Parameter, die erforderlich sind, um eine unbeaufsichtigte Installation in CA Process Automation durchzuführen, sind in der folgende Liste aufgeführt. Parameter, die nicht in diese Liste enthalten sind, sind optional.

Lizenz

thirdPartyLicenseAccepted

licenseAccepted

Installationsverzeichnis

sys.installationDir

Java-Verzeichnis

javaHome

DVD2

domainInstallerDir

Kommunikationsmodus

isSecure (true/false)

Datenbankdetails

- databaseType
- dbUserName
- databaseServer
- databasePortNumber
- libDb
- driver
- runtimeDbType
- runtimeDbUserName
- runtimeDbServer
- runtimeDbPort
- runtimeDb
- runtimeDriver
- reportingDbType
- reportingDbUserName
- reportingDbServer
- reportingDbPort

- reportingDb
- reportingDriver

CA EEM-Details

- registerApplication (für Upgrades als "true" definiert)
- upgradeApplication (für Upgrades als "true" definiert)
- eiamServer
- eiamAppName
- eiamAdminUsrName
- eiamSDKLevel

Neue Parameter für Version 4.2 von CA Process Automation:

nodeCommsV2Port

Der Port, der für den Domänen-Koordinationsrechner für vereinfachte Kommunikation verwendet wird.

eiamSDKLevel

Die Eingabe für die Ebene des CA EEM-SDK.

#hasOracleConnectionString

Gibt an, ob eine Verbindungs-URL angegeben werden soll. Dies gilt nur für Oracle.

#dbOracleConnectionString

JDBC-Verbindungs-URL.

Beispiel:
`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<database host name>) (PORT=<portnumber>)) (CONNECT_DATA=(SERVICE_NAME=<libDb>))).`

Hinweis: Die letzten beiden Eingaben werden dreimal angezeigt; zweimal für jede Datenbank. Diese Parameter sind nur relevant, wenn Sie Oracle als Datenbank auswählen und eine Verbindungszeichenfolge verwenden.

Ausführen oder Bearbeiten der Skriptdatei für die automatische Installation

Nachdem Sie die Antwortdatei erstellt haben, verwenden Sie eine der folgenden Optionen, um die automatische Installation zu starten:

- Führen Sie die Skriptdatei für die automatische Installation aus, und übergeben Sie die Parameter über die Eingabeaufforderung. Diese Option empfiehlt sich wenn Sie einen einzelnen Koordinationsrechner installieren.
- Bearbeiten Sie die Skriptdateiparameter für die Installation, und führen Sie dann das Skript aus. Diese Option empfiehlt sich, wenn Sie mehrere Koordinationsrechner installieren.

Verwenden Sie die Installationsskriptdatei, die für Ihre Betriebsumgebung geeignet ist:

Hinweis: Wenn Sie die Installationsskriptdatei unter UNIX mit einem Dollarzeichens ($) in einem Parameter aufrufen, stellen Sie dem Dollarzeichen ($) einen umgekehrtem Schrägstrich (\) voran. Präfigieren Sie beispielsweise das Datenbankkennwort "abc$123" folgendermaßen mit einem umgekehrten Schrägstrich (\): "abc\$123".

Windows

Syntax

```
Silent_Install_windows.bat [Parameter1] [Parameter2]
[Parameter3]...
```

Verwendung:

```
Silent_Install_windows.bat -VcertPassword=a
-VeiamCertPass=eiamadmin -VeiamPassword=eiamadmin
-VdbPassword=sa -VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

UNIX

Syntax

```
Silent_Install_unix.sh [Parameter1] [Parameter2] [Parameter3]...
```

Verwendung:

```
Silent_Install_unix.sh -VcertPassword=a -VeiamCertPass=eiamadmin
-VeiamPassword=eiamadmin -VdbPassword=sa
-VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

Die Installationsskripten enthalten die folgenden Parameter:

-VcertPassword=*value*

Definiert das Kennwort, das den Zugriff auf die Schlüssel steuert, die Kennwörter verschlüsseln.

-VeiamCertPass

Definiert das CA EEM-Zertifikatskennwort (zum Beispiel "pamadmin").

-VeiamPassword

Gibt das Kennwort für die Datenbank an, die für Automatisierungsobjekte verwendet wird (zum Beispiel "pamadmin").

Hinweis: "VeiamPassword" ist das Windows-Domänenkennwort.

-VdbPassword

Gibt das Kennwort für die Datenbank an, die für die Automatisierung verwendet wird (beispielsweise "objectsroot").

-VreportingDbPassword

Definiert das Kennwort für die Berichtsdatenbank (beispielsweise "root").

-VruntimeDbPassword

Definiert das Kennwort für die Datenbank, die zur Laufzeit verwendet wird (beispielsweise "root").

-VeiamAdminPass

Definiert das Kennwort für den CA EEM-Administrator, wobei der Anwendernamenswert "EiamAdmin" ist (zum Beispiel "eiamadmin").

Wichtig! Kennwortparameter, die über die Befehlszeile übergeben oder in der Skriptdatei für die Installation gespeichert wurden, werden *nicht* verschlüsselt.

Sobald die Installation abgeschlossen ist, können Sie den Koordinationsrechner starten. Überprüfen Sie die Datei "installation.log" nach der Ausführung der Skripts auf Fehler (Installationsverzeichnis\server\c2o).

Hinweise zu Upgrades (automatische Installation)

Bevor Sie ein unbeaufsichtigtes Upgrade auf Version 4.2 von CA Process Automation ausführen, suchen Sie die Datei "response.varfile" Ihrer aktuellen CA Process Automation-Installation.

Diese Datei befindet sich hier:

```
<Installationsverzeichnis>\server\c2o\.install4j\response.varfile
```

Sie benötigen die Werte für die erforderlichen Parameter (siehe Seite 123), um das Upgrade auf Version 4.2 von CA Process Automation vollständig durchzuführen. Sobald Sie diese Werte haben, starten Sie das unbeaufsichtigte Upgrade mit demselben Befehl wie eine Neuinstallation (siehe Seite 125).

Hinweis: jTDS-Treiber sind in Version 4.2 von CA Process Automation obligatorisch. Die Datei "jtds-1.3.1.jar" befindet sich im Ordner "drivers" in DVD1. Sämtliche response.varfile-Parameter aus früheren Installationen, die auf eine SQL JAR-Datei verweisen, müssen in der Datei "response.varfile" für CA Process Automation-Version 4.2 durch einen jTDS-Wert ersetzt werden.

In Version 3.1 von CA Process Automation kann "response.varfile" beispielsweise den folgenden Parameter enthalten:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/sqljdbc.jar
```

In Version 4.2 von CA Process Automation wird dieser Parameter zu:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/jtds-1.3.1.jar
```

Aufgaben nach der Installation für den Domänen-Koordinationsrechner

Führen Sie nach der Installation die anwendbaren Aufgaben aus.

- Wenn Sie den Domänen-Koordinationsrechner neu installiert haben (kein Upgrade durchgeführt), sodass Sie sichere Kommunikation mithilfe von HTTPS festlegen können, dann lesen Sie den Abschnitt Aktivieren der sicheren Kommunikation für ein vorhandenes CA Process Automation (siehe Seite 176).
- Wenn Sie CA Process Automation das erste Mal installiert haben:
  - Überprüfen Sie die Voraussetzungen für die Port-Planung, (siehe Seite 95) um Ports zu konfigurieren.
  - Konfigurieren der Firewalls für bidirektionale Kommunikation (siehe Seite 133).
- Um mit den Datenbankoperatoren eine Verbindung zu Datenbanken mithilfe eines anderen als in CA Process Automation verwendeten RDBMS herzustellen, installieren Sie die Treiber für Datenbankoperatoren (siehe Seite 134).

  Um Windows-Authentifizierung (integrierte Sicherheit) mit JDBC für MSSQL Server zu verwenden, installieren Sie Treiber für Datenbankoperatoren (siehe Seite 134).
- Wenn Sie den Domänen-Koordinationsrechner auf einem Server mit dem Betriebssystem HP-UX installiert haben, führen Sie zusätzliche Konfigurationsschritte auf HP-UX aus.
- Wenn Sie CA EEM mit Microsoft Active Directory als das externe Verzeichnis installiert haben, kann CA EEM Anwender mithilfe des NTLM-Protokolls authentifizieren. Wenn Sie sich nicht für die NTLM-Durchleitungs-Authentifizierung während der Installation entschieden haben, können Sie dies nun manuell vornehmen. Siehe Aktivieren der NTLM-Durchleitungs-Authentifizierung nach der Installation (siehe Seite 135).
- Für Aufgaben, wie das Bereitstellen von Treibern für Datenbankoperatoren, ist es erforderlich, dass Sie den Domänen-Koordinationsrechner neu starten.
  - Weitere Informationen finden Sie unter Anhalten des Koordinationsrechners (siehe Seite 142).
  - Weitere Informationen finden Sie unter Starten des Koordinationsrechners (siehe Seite 143).
- Bevor Sie den ersten Administrator in CA EEM konfigurieren, können Sie zu CA Process Automation navigieren und sich als standardmäßiger Administrator anmelden.

  Weitere Informationen finden Sie unter Navigieren zu CA Process Automation und Anmelden als standardmäßiger Administrator (siehe Seite 129).

Navigieren zu CA Process Automation und Anmelden als standardmäßiger Administrator

Viele Themen in diesem Handbuch setzen voraus, dass Sie Zugriff auf die CA Process Automation-Anwenderoberfläche haben. Aufgaben, wie das Bereitstellen von Treibern, Installieren von Koordinationsrechnern und Hinzufügen von Knoten, werden über die Registerkarte "Konfiguration" in CA Process Automation initiiert. Administratoren melden sich normalerweise bei CA Process Automation mit ihren eigenen Anmeldeinformationen an, um solche Aufgaben auszuführen.

Hinweis: Weitere Informationen über das Erstellen Ihres eigenen Anwenderkontos finden Sie im *Handbuch für Inhaltsadministratoren*.

Um verfügbar zu sein, erfordert CA Process Automation, dass die folgenden Bedingungen erfüllt werden:

- CA EEM wird ausgeführt.
- Wenn der Lastenausgleich verwendet wird, sollte dieser ausgeführt werden.
- Der Service des Domänen-Koordinationsrechners ist gestartet. Weitere Informationen finden Sie unter Starten des Koordinationsrechners (siehe Seite 143).

Wenn Sie Aufgaben ausführen möchten, für die der Zugriff auf CA Process Automation erforderlich ist und Sie kein CA Process Automation-Anwenderkonto haben, können Sie sich bei CA Process Automation mit den Anmeldeinformationen eines standardmäßigen Administrators anmelden.

Wichtig! Standardmäßige Administrator-Anmeldeinformationen sind nicht verfügbar, wenn CA EEM für die Verwendung von Microsoft Active Directory als Anwenderspeicher konfiguriert ist. Standardmäßige Anmeldeinformationen für alle Anwenderrollen sind nur verfügbar, wenn Sie CA EEM so konfiguriert haben, dass zum Erstellen und Speichern von Anwenderkonten der lokale Anwenderspeicher verwendet wird.

Gehen Sie folgendermaßen vor:

1. Greifen Sie auf die entsprechende CA Process Automation-URL zu. In den folgenden Beispielen bezieht sich *Server* auf den Server, auf dem ein nicht geclusterter Domänen-Koordinationsrechner installiert ist. Für einen geclusterten Domänen-Koordinationsrechner, bezieht sich *server* auf den Server mit dem Lastenausgleich.

   - Verwenden Sie für sichere Kommunikation die folgende Syntax:

     `https://server:port/itpam`

     Beispiele:

     `https://domainOrchestrator_host:8443/itpam`

     `https://loadBalancer_host:443/itpam`

   - Verwenden Sie für einfache Kommunikation die folgende Syntax:

     `http://server:port/itpam`

     Beispiele:

     `http://domainOrchestrator_host:8080/itpam`

     `http://loadBalancer_host:80/itpam`

   Die Anmeldeseite von CA Process Automation wird geöffnet.

   Hinweis: Wenn die NTLM-Authentifizierung aktiviert ist und Ihre Domänen-Anmeldeinformationen mit den Anmeldeinformationen in einem CA EEM-Anwenderkonto übereinstimmen, wird die Registerkarte "Startseite" angezeigt. Um die NTLM-Authentifizierung in Mozilla Firefox zu unterstützen, müssen Sie die Browsereinstellungen konfigurieren. Weitere Informationen sind dem Mozilla-Support zu entnehmen.

2. Geben Sie **pamadmin** als Anwendernamen ein.

3. Geben Sie **pamadmin** als Kennwort ein.
4. Klicken Sie auf Anmelden.

   CA Process Automation wird geöffnet. Die Registerkarte "Startseite" wird angezeigt.
5. Klicken Sie in der Drop-down-Liste "Hilfe" auf "Bookshelf". Stellen Sie sicher, dass das Bookshelf über den Kunden-Support von CA Technologies geöffnet werden kann.
6. Wenn sich das Bookshelf nicht öffnet, weil in der Umgebung, in der CA Process Automation-Anwender arbeiten, kein Internetzugriff besteht, gehen Sie folgendermaßen vor:
   a. Gehen Sie zu einem Unternehmensstandort mit Internetzugriff.
   b. Durchsuchen Sie das System nach der URL des Bookshelf für CA Process Automation Release 04.20.00 https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html.
   c. Klicken Sie auf den Link "Dieses Bookshelf herunterladen".
   d. Verschieben Sie das Bookshelf aus dem Download-Verzeichnis nach:

Verfügbarmachen des Bookshelf für Anwender ohne Internetzugriff

Anwender mit Internetzugriff können das Bookshelf mit der CA Process Automation-Dokumentation über den Link "Bookshelf" in CA Process Automation öffnen. Dieser Link greift auf das Bookshelf für Version 4.2 von CA Process Automation im Kunden-Support von CA Technologies zu.

Anwender ohne Internetzugriff benötigen Ihre Hilfe, um auf das CA Process Automation-Bookshelf zugreifen zu können. Aktivieren Sie den Bookshelf-Link, indem Sie das Bookshelf herunterladen und in einen Speicherort verschieben, aus dem die Kopie auf dem lokalen Server entnommen werden soll.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA Process Automation und, und melden Sie sich als standardmäßiger Administrator an (siehe Seite 129).
2. Klicken Sie in der Drop-down-Liste "Hilfe" auf "Bookshelf". Überprüfen Sie, ob das Bookshelf über den Kunden-Support von CA Technologies geöffnet werden kann.

3. Wenn sich das Bookshelf nicht öffnet, weil in der Umgebung, in der CA Process Automation-Anwender arbeiten, kein Internetzugriff besteht, gehen Sie folgendermaßen vor:
   a. Gehen Sie zu einem Unternehmensstandort mit Internetzugriff.
   b. Durchsuchen Sie das System nach der URL des Bookshelf für CA Process Automation Release 04.20.00 https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html.
   c. Klicken Sie auf den Link "Dieses Bookshelf herunterladen".
   d. Verschieben Sie das Bookshelf aus dem Download-Verzeichnis nach:

      ```
      Installationsverzeichnis\server\c2o\.c2orepository\bookshelf
      ```

4. Klicken Sie in der Drop-down-Liste "Hilfe" auf "Bookshelf". Überprüfen Sie, ob das Bookshelf geöffnet wird.

Konfigurieren der Firewalls für bidirektionale Kommunikation

CA Process Automation-Komponenten sind über Web-Clients zugreifbar. In Von CA Process Automation verwendete Ports (siehe Seite 231) finden Sie Details zu den Ports, die von den einzelnen Komponenten in einem CA Process Automation-System verwendet werden.

Sie müssen Firewalls konfigurieren, um Birichtungskommunikation zu ermöglichen. Birichtungskommunikation wird zwischen den folgenden Komponentenpaaren benötigt:

- Der Domänen-Koordinationsrechner und der Datenbankserver, die für die Bibliotheksdatenbank verwendet werden.
- Der Domänen-Koordinationsrechner und der Datenbankserver, die für die Berichtsdatenbank verwendet werden.
- Der Domänen-Koordinationsrechner und der Datenbankserver, die für die Laufzeitdatenbank verwendet werden.
- Der Domänen-Koordinationsrechner und CA EEM.
- Jeder Koordinationsrechner und der Datenbankserver, die für die Bibliotheksdatenbank verwendet werden.
- Jeder Koordinationsrechner und der Datenbankserver, die für die Berichtsdatenbank verwendet werden.
- Jeder Koordinationsrechner und der Datenbankserver, die für die Laufzeitdatenbank verwendet werden.

Wenn Sie lokale Firewalls auf Koordinationsrechner- oder Agenten-Hostcomputern verwenden, stellen Sie sicher, dass ausführbare CA Process Automation-Dateien fähig sind, zu empfangen und eine bidirektionale Verbindung über die Firewall auf den einzelnen Hosts herzustellen. Einige hostbasierte Firewallprogramme (z. B. die Windows-Firewall) lassen Ausnahmen für ausführbare Dateien zu.

Installieren der Treiber für Datenbankoperatoren

CA Process Automation-Designer können Operatoren von der Kategorie "Datenbank" verwenden (früher JDBC-Modul), um eine Verbindung mit verschiedenen RDBMS (Relational Database Management Systems) herzustellen. Wenn die Verbindung zu einer MySQL-Datenbank, einer Oracle-Datenbank oder einer Microsoft SQL Server-Datenbank hergestellt ist, sind die richtigen Treiber verfügbar. (Die Verfügbarkeit von allen drei Treibern hängt von Ihrer Auswahl ab, die Sie während der Installation des Domänen-Koordinationsrechners vornehmen.) Wenn die Verbindung zu einer Datenbank durch einen anderen Anbieter hergestellt ist, können Sie den JDBC-Treiber für Datenbankoperatoren für diese Datenbank auf der Registerkarte der CA Process Automation-Konfiguration bereitstellen. Wenn ein Designer beispielsweise die Datenbankoperatoren für Sybase verwenden möchte, stellt ein Administrator die JDBC-Treiber für Sybase bereit. Ein Administrator kann JDBC-Treiber auf Koordinationsrechnern oder auf Hosts mit CA Process Automation-Agenten bereitstellen.

Hinweis: Informationen zu den Vorgängen finden Sie unter So stellen Sie JDBC-Treiber für Datenbankoperatoren bereit im Kapitel "Verwalten von Anwenderressourcen" im *Handbuch für Inhaltsadministratoren.*

Aktivieren der NTLM-Durchleitungs-Authentifizierung nach der Installation

NTLM-Durchleitungs-Authentifizierung aktiviert CA EEM, um Anwender mithilfe des NTLM-Protokolls zu authentifizieren. Dies ist eine Alternative zur Verwendung von Anmeldeinformationen, die Anwender in ein formularbasiertes Anmeldedialogfeld eingeben. Mit der NTLM-Durchleitungs-Authentifizierung wird das Anmeldedialogfeld übersprungen.

Der folgende Vorgang gilt *nicht*, wenn Sie bereits NTLM-Durchleitungs-Authentifizierung aktiviert haben, zum Beispiel:

- Sie haben während der interaktiven Installation von CA Process Automation die Option "NTLM-Durchleitungs-Authentifizierung aktivieren" ausgewählt.
- Sie haben "enableNTLM=true" in der Datei "response.varfile" angegeben, die für die automatische Installation von CA Process Automation verwendet wurde.

Sie können NTLM-Durchleitungs-Authentifizierung aktivieren, indem Sie "ntlm.enabled=true" der Datei "OasisConfig.properties" manuell hinzufügen. Verwenden Sie folgenden Vorgang nur dann, wenn Sie diese Funktion aktivieren möchten und sie bei der Installation nicht aktiviert haben.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
2. Navigieren Sie zum folgenden Ordner, wobei "Installationsverzeichnis" für den Installationspfad des Domänen-Koordinationsrechners steht:

   `Installationsverzeichnis/server/c2o/.config`
3. Öffnen Sie die Datei "OasisConfig.properties" mit einem Editor.
4. Verwenden Sie "Suchen", um folgende Eigenschaft zu finden: ntlm.enabled=
5. Ändern Sie den Wert für die Eigenschaft auf "true", das bedeutet auf:

   `ntlm.enabled=true`
6. Speichern Sie die Datei, und schließen Sie den Editor.
7. Starten Sie den Koordinationsrechner-Service neu.
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 142).
   b. Starten Sie den Koordinationsrechner (siehe Seite 143).
8. Wiederholen Sie diesen Prozess für jeden Koordinationsrechner.

Interaktion mit der Desktop-Konfiguration

Koordinationsrechner und Agenten werden normalerweise als Konsolendienste ausgeführt und müssen nicht mit dem Desktop interagieren. Wenn ein Koordinationsrechner oder Agent mit dem Windows-Desktop interagieren muss, muss der Koordinationsrechner- oder Agentendienst mithilfe des Anwenderkontos oder mithilfe des Kontos "Lokales System" mit der aktivierten Option "Interaktion des Dienstes mit dem Desktop zulassen" gestartet werden. Diese Option ist standardmäßig aktiviert, wenn ein Koordinationsrechner oder Agent installiert wird. Alternativ kann dieser Dienst auch mithilfe der Dienstekonsole in der Windows-Verwaltung konfiguriert werden. Das Kontrollkästchen zum Erteilen dieser Berechtigung befindet sich auf der Registerkarte "Anmelden" des Eigenschaftsfensters für den Dienst.

Weitere Informationen finden Sie unter Konfigurieren von CA EEM, um es referenzierten Anwendern zu ermöglichen, sich mit ihrem E-Mail-Namen anzumelden

Wenn Sie CA Process Automation installieren, können Sie "Globale Benutzer/Globale Gruppen" in der EEM-Serverkonfiguration als "Referenz" aus einem externen Verzeichnis konfigurieren. Sie können dann mehrere Active Directory-Domänen auswählen und die Microsoft Active Directorys (ADs) angeben, in denen potenzielle CA Process Automation-Anwender definiert sind. Während einer CA Process Automation-Installation identifizieren Sie die standardmäßige AD-Domäne. Anwender, die zum standardmäßigen AD gehören, können sich mit ihrem Anwendernamen und ihrem Kennwort bei CA Process Automation anmelden. Anwender, die zu anderen AD-Domänen gehören, müssen ihren Prinzipalnamen und ihr Kennwort bei der Anmeldung eingeben. Das standardmäßige Formular für einen Prinzipalnamen ist *Domäne\Anwendername*.

Sie können CA EEM konfigurieren, um die Active Directory-Anwender mit ihrer E-Mail-Adresse, *Anwendername@Domäne*, zu authentifizieren. Sie konfigurieren CA EEM, um mithilfe von "userPrincipalName" nach dem Anwender zu suchen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei CA EEM als CA EEM-Administrator an, und wählen Sie den Anwendungsnamen aus, den Sie während der CA Process Automation-Installation festlegen.
2. Wählen Sie die Registerkarte "Konfigurieren" aus.
3. Wählen Sie im Auswahlmenü "Benutzerspeicher" die Option "LDAP-Attributzuordnung" aus.

4. Erstellen Sie eine Attributzuordnung von der vorhandenen Attributzuordnung, indem Sie den Anwenderauthentifizierungsfilter ändern. Das heißt, ändern Sie "samaccountName" in "userPrinciaplName".

   a. Wählen Sie "Microsoft Active Directory" aus der Dropdown-Liste "Zuordnungsname" aus.

   b. Im Bereich "Benutzersuche" ist der Benutzersuchfilter dem folgenden Beispiel ähnlich:

      ```
      (&(objectClass=user)(!(objectClass=computer)))
      ```

   c. Bearbeiten Sie das Feld "Benutzerauthentifizierungsfilter" so, dass "userPrincipalName" den Wert "samaccountName" ersetzt. Sehen Sie sich folgende Beispielergebnisse an:

      ```
      (&(ObjectClass=user)(!(objectClass=computer)(userPrincipalName= ...
      ```

   d. {UserName} ist folgendermaßen festgelegt:

      ```
      ))
      ```

5. Speichern Sie die Attributzuordnung. Geben Sie zum Beispiel den Namen "**madAuthMail**" im Feld "Zuordnungsname" ein, und klicken Sie dann auf "Speichern".

6. Die Daten der Benutzerattributzuordnung ähneln folgenden Daten:

   Anwendername: sAMAccountName

   Vorname: givenName

   Nachname: sn

   Anzeigename: displayName

7. Geben Sie unter "Konfiguration des LDAP-Verzeichnisses" im Abschnitt "Allgemein" den Namen der Attributzuordnung ein, den Sie in Schritt 5 erstellt haben. Überprüfen Sie, ob Ihre Eingaben dem folgenden Text ähneln:

   Name: *domain*

   Attributzuordnung: madAuthMail

   Domäne: *domain*

   Ausgewählte Hostnamen: *hostname:*389

   Protokoll: LDAP

   Basis-DN: ou=*mylocation*,dc=*mycompany*,dc=com

   Anwender-DN: cn=*userid*,ou=Users,ou=*mylocation*,dc=*mycompany*,dc=com

   Anwenderkennwort: *passwordForUserid*

Voraussetzungen der Zeitsynchronisierung

Es ist empfehlenswert, die Uhrzeit des Domänen-Koordinationsrechners mit einem standardmäßigen externen Zeitserver zu synchronisieren. Dies bereitet den Domänen-Koordinationsrechner auf den Zeitpunkt vor, wenn ein Cluster-Knoten hinzugefügt wird. Alle Cluster-Knoten für einen Koordinationsrechner müssen die gleiche Uhrzeit haben, idealerweise mit einem standardmäßigen externen Zeitserver synchronisiert. Der Lastenausgleich verarbeitet die Zeitsynchronisierung nicht.

Weitere Informationen:

Synchronisieren der Zeit für einen Cluster-Knoten (siehe Seite 199)

Installieren von Patches und Connectors mit CA Process Automation 4.2

Dieser Abschnitt beschreibt, wie CA Process Automation-Connectors mit JBoss 5.1 auf einem Host installiert werden.

Administratoren können die CA Process Automation-Connectors installieren, um es CA Process Automation zu ermöglichen, mit anderen Produkten (CA-Produkte und Produkte von Drittanbietern) zu interagieren, um Geschäftsanwendungsfälle zu automatisieren. Jeder Connector agiert als Modul, das eine Reihe von Operatoren enthält. Die Operatoren interagieren mit APIs von anderen Produkten und werden verwendet, um CA Process Automation-Abläufe zu erstellen.

Stellen Sie als Voraussetzung sicher, dass CA Process Automation auf dem Host installiert ist. Die ausführbare Datei des CA Process Automation-Connectors ist auf dem Host vorhanden.

Wichtig! Um CA Process Automation-Patch und -Connector erfolgreich zu installieren, fahren Sie alle Koordinationsrechner-Knoten herunten, und installieren Sie CA Process Automation-Patch und -Connector auf allen Knoten (Domänenknoten und solche, bei denen es sich nicht um Domänenknoten handelt).

Gehen Sie folgendermaßen vor:

1. Führen Sie die ausführbare Datei des CA Process Automation-Connectors aus.

   Die Willkommenseite wird angezeigt.

2. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".

3. Geben Sie auf der Seite "Wählen Sie ein CA Process Automation-Installationsverzeichnis aus" den Speicherort des *Installationsverzeichnisses* an.

4. Wählen Sie auf der Seite "Connectors zum Installieren/Aktualisieren auswählen" die Connectors aus, die installiert werden sollen, und klicken Sie auf "Weiter".

   Der CA Process Automation-Connector wird installiert.

5. Um die Installation des CA Process Automation-Connector zu überprüfen, navigieren Sie zu CA Process Automation, und melden Sie sich an. Klicken Sie auf die Registerkarte "Designer" und anschließend auf "Neuer Prozess".

   Der installierte CA Process Automation-Connector mit seinen Operatoren wird in der Ansicht "Operatoren" aufgelistet.

Ändern der Konfiguration des Oracle-Datenbankservers für die Verwendung von Oracle RAC

Sie können den Oracle-Datenbankserver, den Sie für CA Process Automation einrichten und während der CA Process Automation-Installation konfiguriert haben, weiterhin verwenden. Wenn dieser eigenständige Oracle-Server Teil eines Oracle Real Application Cluster ist, können Sie nach der Installation optional Oracle RAC als Datenbankserver konfigurieren.

Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass CA Process Automation den konfigurierten eigenständigen Oracle-Datenbankserver, der bei der Installation für Bibliotheksdatenbank, Laufzeitdatenbank und Berichtsdatenbank angegeben wurde, erfolgreich verwendet.
2. Halten Sie den CA Process Automation-Service an. Die entsprechende Beschreibung finden Sie unter Anhalten des Koordinationsrechners (siehe Seite 142).
3. Öffnen Sie die Datei "OasisConfig.properties".

   Installationsverzeichnis\server\c2o\.config\OasisConfig.properties
4. Ändern Sie die folgenden Eingaben für die Bibliotheksdatenbank:

   oasis.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.database.lib.dbname=*ServiceName*
   oasis.database.queues.dbname=*ServiceName*
   oasis.database.dbhostname=*Oracle-RAC*
5. Ändern Sie die folgenden Eingaben für die Laufzeitdatenbank:

   oasis.runtime.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.runtime.database.dbname=*ServiceName*
   oasis.runtime.database.dbhostname=*Oracle-RAC*
6. Ändern Sie die folgenden Eingaben für die Berichtsdatenbank:

   oasis.reporting.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.reporting.database.dbname=*ServiceName*
   oasis.reporting.database.dbhostname=*Oracle-RAC*
7. Speichern Sie die Datei "OasisConfig.properties".
8. Starten Sie den Koordinationsrechner (siehe Seite 143).

Hinweis: Für die Anweisungen für die Verbindungs-URL gelten die folgenden Notationen ebenfalls:

TNS-Notation

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ora
cle-server)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ServiceName)
))
```

RAC-TNS-Notation

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=OFF)(FAILOVER=ON)(
ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1
521))(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1521)))(C
ONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=ServiceName)))
```

Andere Notation (keine Schrägstriche; Anweisung endet mit Doppelpunkt)

```
jdbc:oracle:thin:@oracle-server:1521:
```

Anhalten des Koordinationsrechners

Nur Administratoren mit Administratoren-Anmeldeinformationen auf dem Server, auf dem der Koordinationsrechner installiert ist, können den Koordinationsrechner anhalten.

Wichtig! Wenn ein Koordinationsrechner nicht ordnungsgemäß heruntergefahren wird, können sich im folgenden temporären Ordner Dateien mit einem Volumen von mehreren GB anhäufen. Wenn dies geschieht, können Sie den folgenden temporären Ordner ohne Bedenken löschen:

Installationsverzeichnis/server/c2o/tmp

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Koordinationsrechner installiert ist.
2. Wenn Sie bei einem Windows-Host angemeldet sind, können Sie den Koordinationsrechner-Service vom Startmenü, über das Fenster "Dienste" oder von der Befehlszeile aus anhalten. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im Startmenü die Option "Programme", "CA", "CA Process Automation 4.0" und "Koordinationsrechner-Service anhalten" aus.
   - Wählen Sie in der Systemsteuerung die Option "Verwaltung" und dann "Dienste". Wählen Sie die folgenden Service aus, und klicken Sie auf "Ende".

     CA Process Automation-Koordinationsrechner (C:\Programme\CA\PAM\server\c2o)
   - Öffnen Sie eine Eingabeaufforderung, und führen Sie das folgende Skript aus:

     Installationsverzeichnis/server/c2o/bin/stopc2osvc.bat
3. Wenn Sie auf einem UNIX- oder Linux-Host angemeldet sind, führen Sie folgende Schritte aus:
   a. Wechseln Sie die Verzeichnisse zu "${PAM_HOME}/server/c2o/". Ändern Sie zum Beispiel Verzeichnisse zu:

      /usr/local/CA/PAM/server/c2o
   b. Führen Sie das Skript "c2osvrd.sh" mit der Option "stop" aus. Zum Beispiel:

      ./c2osvrd.sh stop

Starten des Koordinationsrechners

Nur Administratoren mit Administratoren-Anmeldeinformationen auf dem Server, auf dem der Koordinationsrechner installiert ist, können den Koordinationsrechner-Service neu starten.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Koordinationsrechner installiert ist.
2. Wenn Sie bei einem Windows-Host angemeldet sind, können Sie den Koordinationsrechner-Service vom Startmenü, über das Fenster "Dienste" oder von der Befehlszeile aus neu starten. Führen Sie eine der folgenden Aufgaben aus:
   - Wählen Sie im Startmenü die Option "Programme", "CA", "CA Process Automation" und "Koordinationsrechner-Service starten" aus.
   - Wählen Sie in der Systemsteuerung die Option "Verwaltung" und dann "Dienste". Wählen Sie den folgenden Service aus, und klicken Sie auf "Start".

     `CA Process Automation-Koordinationsrechner (C:\Programme\CA\PAM\server\c2o)`
   - Öffnen Sie eine Eingabeaufforderung, und führen Sie das folgende Skript aus:

     `Installationsverzeichnis``/server/c2o/bin/startc2osvc.bat`
3. Wenn Sie auf einem UNIX- oder Linux-Host angemeldet sind, führen Sie folgende Aufgaben aus:
   a. Wechseln Sie die Verzeichnisse zu "${PAM_HOME}/server/c2o/". Ändern Sie zum Beispiel Verzeichnisse zu:

      `/usr/local/CA/PAM/server/c2o`
   b. Führen Sie das Skript "c2osvrd.sh" mit der Option "start" aus. Führen Sie daher Folgendes aus:

      `./c2osvrd.sh start`

Hinweis: Nachdem Sie den Service für den Domänen-Koordinationsrechner gestartet haben, starten Sie CA Process Automation.

Deinstallieren des Domänen-Koordinationsrechners

Nur Administratoren mit Administratoren-Anmeldeinformationen auf dem Server, auf dem der Domänen-Koordinationsrechner installiert ist, können den Koordinationsrechner deinstallieren.

Hinweis: Halten Sie den Domänen-Koordinationsrechner an, bevor Sie ihn deinstallieren.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Domänen-Koordinationsrechner installiert ist.
2. Wenn Sie sich bei den folgenden Hosts angemeldet haben:
   a. Ein Windows-Host:
   Sie können den Domänen-Koordinationsrechner über das Startmenü und die Systemsteuerung deinstallieren. Führen Sie eine der folgenden Aufgaben aus:
      - Wählen Sie im Startmenü die Option "Programme", "CA", "CA Process Automation 4.2" und "CA Process Automation deinstallieren" aus.
      - Wählen Sie im Startmenü die Option "CA Process Automation-Domäne", "Systemsteuerung", "Programme und Funktionen" aus, und klicken Sie auf "Deinstallieren".

        Der Deinstallationsassistent wird angezeigt.

   b. Ein UNIX- oder Linux-Host führt folgende Aufgaben durch:
      a. Ändern Sie die Verzeichnisse in "${PAM_STARTVERZEICHNIS}/standalone/" um. Ändern Sie zum Beispiel Verzeichnisse zu:

         ```
         /usr/local/CA/PAM/server/c2o
         ```

      b. Führen Sie das Skript "./uninstall" aus.

         Der Deinstallationsassistent wird angezeigt.
3. Nachdem der Domänen-Koordinationsrechner deinstalliert wurde, überprüfen Sie folgende Änderungen:
   - Der Dienst "CA Process Automation-Domäne" wird in der Systemsteuerung unter "Verwaltung" und "Dienste" gelöscht.
   - Die Eingabe "CA Process Automation-Domäne" wird im Startmenü unter "Systemsteuerung", "Programme und Funktionen" entfernt.
   - Der Ordner "Domänen-Koordinationsrechner" wird aus dem Installationsspeicherort entfernt.

Kapitel 6: Upgrade auf die aktuelle Version

Sie können ein Upgrade von Version 4.2 von CA Process Automation auf die folgenden Versionen von CA Process Automation durchführen:

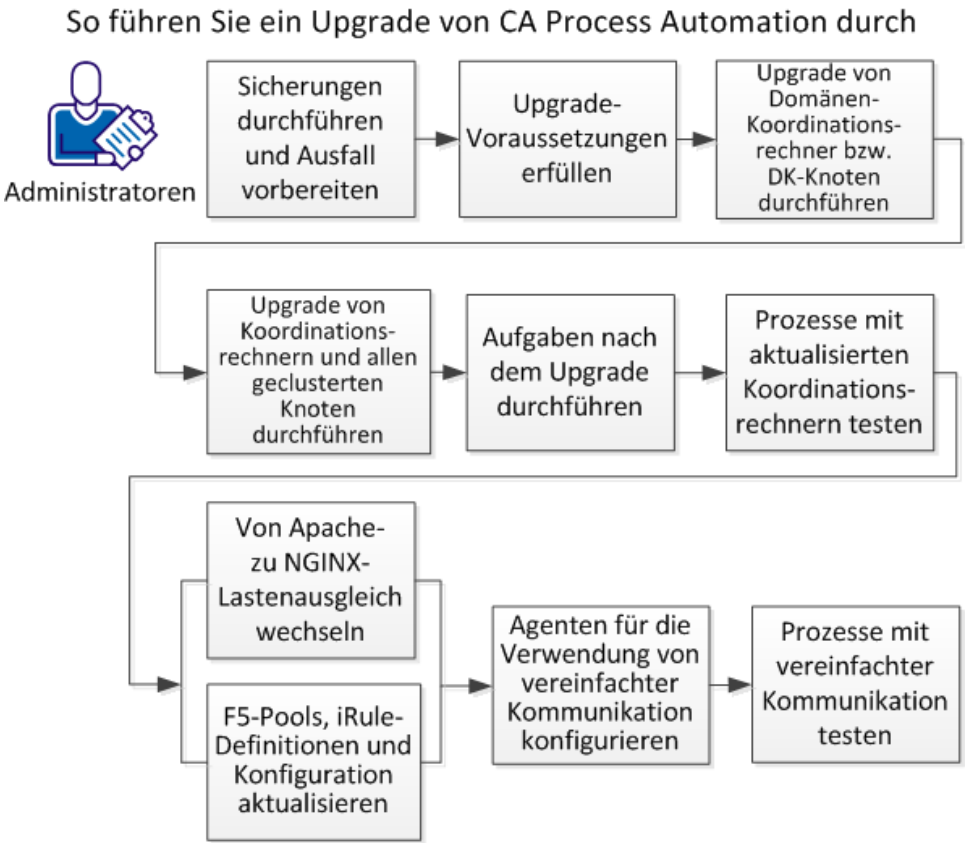
- CA Process Automation 3.1 SP01
- CA Process Automation 4.0 SP01
- CA Process Automation Version 4.1
- CA Process Automation 4.1 SP01

Dieses Kapitel enthält folgende Themen:

So führen Sie ein Upgrade von CA Process Automation durch (siehe Seite 146)
Durchführen von Sicherungen und Vorbereiten des Ausfalls (siehe Seite 147)
Erfüllen von Upgrade-Voraussetzungen (siehe Seite 149)
Durchführen eines Upgrade des Domänen-Koordinationsrechners (siehe Seite 150)
Durchführen eines Upgrade eines nicht geclusterten Koordinationsrechners (siehe Seite 155)
Durchführen eines Upgrade eines Cluster-Knoten (siehe Seite 158)
Ausführen von Aufgaben nach dem Upgrade (siehe Seite 161)
Testen der Prozesse mit den aktualisierten Koordinationsrechnern (siehe Seite 162)
Wechseln von Apache- zu NGINX-Lastenausgleich (siehe Seite 163)
Aktualisieren von F5-Pools, iRule-Definition und Konfiguration (siehe Seite 163)
Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation (siehe Seite 164)
Testen der Prozesse mit vereinfachter Kommunikation (siehe Seite 165)

So führen Sie ein Upgrade von CA Process Automation durch

Für Upgrades von Version 3.1 SP01 und höher auf Version 4.2 von CA Process Automation können Sie dem dargestellten Prozess folgen.


So führen Sie ein Upgrade von CA Process Automation durch
Administratoren
Sicherungen durchführen und Ausfall vorbereiten
Upgrade-Voraussetzungen erfüllen
Upgrade von Domänen-Koordinations-rechner bzw. DK-Knoten durchführen
Upgrade von Koordinations-rechnern und allen geclusterten Knoten durchführen
Aufgaben nach dem Upgrade durchführen
Prozesse mit aktualisierten Koordinations-rechnern testen
Von Apache- zu NGINX-Lastenausgleich wechseln
F5-Pools, iRule-Definitionen und Konfiguration aktualisieren
Agenten für die Verwendung von vereinfachter Kommunikation konfigurieren
Prozesse mit vereinfachter Kommunikation testen

Wichtig! Führen Sie bei Bedarf ein Upgrade von einer Version vor r3.1 SP01 (siehe Seite 305) durch, bevor Sie den hier dokumentierten Prozess starten.

Gehen Sie folgendermaßen vor:

1. Führen Sie Sicherungen durch, und bereiten Sie den Ausfall vor (siehe Seite 147).
2. Erfüllen Sie die Upgrade-Voraussetzungen (siehe Seite 149).
3. Führen Sie ein Upgrade des Domänen-Koordinationsrechners durch (siehe Seite 150).
4. Führen Sie Upgrades weiterer Koordinationsrechner und aller geclusterten Knoten Upgrade durch.
   - Führen Sie ein Upgrade eines nicht geclusterten Koordinationsrechners durch (siehe Seite 155).
   - Führen Sie ein Upgrade eines Cluster-Knotens durch (siehe Seite 158).
5. Führen Sie Aufgaben nach dem Upgrade durch (siehe Seite 161).
6. Testen Sie Ihre Prozesse mit den aktualisierten Koordinationsrechnern (siehe Seite 162).
7. Eine der folgenden Komponenten:
   - Wechseln Sie von Apache- zu NGINX-Lastenausgleich (siehe Seite 163).
   - Aktualisieren Sie F5-Pools, iRule-Definition und Konfiguration (siehe Seite 163).
8. Konfigurieren Sie Agenten für die Verwendung von vereinfachter Kommunikation (siehe Seite 164).
9. Testen Sie Ihre Prozesse mit vereinfachter Kommunikation (siehe Seite 165).

Durchführen von Sicherungen und Vorbereiten des Ausfalls

Unvorhergesehene oder nicht steuerbare Vorfälle können den Upgrade-Prozess unterbrechen oder anderweitig fehlschlagen lassen. Es wird empfohlen, Sicherheitskopien aller wertvollen Daten, die in CA Process Automation-Ordnern gespeichert sind, zu erstellen, bevor Sie mit dem Upgrade beginnen. Als Vorbereitung auf eine vollständige Zurückführung erstellen Sie auch Sicherheitskopien von CA Process Automation-Inhalten, die in Ihren Datenbankservern und in CA EEM gespeichert sind.

Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass Ihre Datenbankserver über einen Speicherplatz verfügen, der mindestens der doppelten Größe entspricht, die derzeit von Ihren vorhandenen CA Process Automation-Datenbanken belegt wird.

2. Um sich auf eine potenzielle Zurückführung vorzubereiten, erstellen Sie Snapshots aller Koordinationsrechner-VMs, oder erstellen Sie Sicherheitskopien des folgenden Ordners, der sich auf allen Koordinationsrechnern befindet:

   Installationsverzeichnis/server/c2o/

   Die Best Practice besteht darin, diesen Ordner auf einem anderen physischen Datenträger zu sichern als jenem, auf dem sich der Ordner *Installationsverzeichnis* befindet.

3. Erstellen Sie vor dem Upgrade Sicherheitskopien aller Bibliotheks-, Laufzeit- und Berichtsdatenspeicher, die von Koordinationsrechnern verwendet werden. Datenspeicher können sich in separaten Datenbankservern oder im selben Datenbankserver befinden.

4. Erstellen Sie eine Sicherheitskopie der CA Process Automation-Anwendung in Ihrem CA EEM-Server.

   a. Melden Sie sich unter Angabe der CA Process Automation-Anwendung bei CA EEM an.

   b. Klicken Sie auf die Registerkarte "Konfigurieren" und anschließend auf "EEM-Server" und "Anwendung exportieren".

   c. Klicken Sie auf "Exportieren", und speichern Sie die Datei <Anwendungsname>.gz auf Ihrem lokalen Laufwerk.

5. Bereiten Sie sich auf einen Ausfall vor. Die Dauer eines Koordinationsrechner-Upgrade hängt von der Größe der Datenspeicher ab. Je mehr Daten Sie haben, desto mehr Zeit nimmt das Upgrade in Anspruch.

   - Wenn Sie weitere Anwendungen verwenden, die von CA Process Automation-Services abhängen, bereiten Sie sich auf diesen Ausfall vor. Wenn Sie beispielsweise Service Catalog mit CA Process Automation-Prozessen verwenden, könnten Sie Service Catalog während des CA Process Automation-Upgrade herunterfahren. Alternativ könnten Sie für Katalogelemente, die von CA Process Automation abhängen, ein Dialogfeld der Art "Vorübergehend nicht verfügbar" verwenden, das sie nach Abschluss des CA Process Automation-Upgrade wieder entfernen.

   - Planen Sie ein realistisches Wartungsfenster, und informieren Sie relevante Stakeholder über den Zeitraum, während dessen CA Process Automation voraussichtlich nicht verfügbar ist.

Erfüllen von Upgrade-Voraussetzungen

Bevor Sie den Prozess zum Upgrade auf CA Process Automation Version 04.2.00 durchführen, müssen Sie folgende erforderliche Aufgaben erfüllen:

1. Halten Sie die Administrator-Anmeldeinformationen für CA EEM bereit. Üblicherweise ist der Anwendername des EEM-Admin "EiamAdmin", und der CA EEM-Administratir kennt das EEM-Admin-Kennwort.
2. Notieren Sie das Zertifikatskennwort, das für dieses System-Upgrade verwendet werden soll.

   Das Zertifikatskennwort wird verwendet, um den Zugriff auf die Schlüssel zu steuern, die verwendet werden, um Kennwörter und andere kritische Daten zu verschlüsseln. Sie geben dieses Kennwort für den ersten Koordinationsrechner an, für den Sie ein Upgrade durchführen. Wenn Sie weitere Knoten des Domänen-Koordinationsrechners, andere eigenständige Koordinationsrechner oder Knoten anderer geclusterter Koordinationsrechner für dieselbe Version installieren, müssen Sie dasselbe Kennwort angeben.

   Wichtig! Sie müssen dasselbe Zertifikatskennwort verwenden, das in der Version verwendet wurde, von der Sie das Upgrade durchführen.
3. Stellen Sie sicher, dass derzeit keine CA Process Automation-Prozesse aktiv sind, d. h. sich im Status "Wird ausgeführt" oder "Blockiert" befinden.
4. Fahren Sie alle Nicht-Domänen-Koordinationsrechner herunter. Fahren Sie bei einem geclusterten Nicht-Domänen-Koordinationsrechner den Koordinationsrechner-Service auf jedem Knoten herunter. Weitere Informationen finden Sie unter Anhalten des Koordinationsrechners (siehe Seite 142).
5. Fahren Sie den Domänen-Koordinationsrechner herunter. Fahren Sie bei einem geclusterten Domänen-Koordinationsrechner den Koordinationsrechner-Service auf jedem Knoten herunter. Weitere Informationen finden Sie unter Anhalten des Koordinationsrechners (siehe Seite 142).

   Hinweise:

   - Aktive Agenten können keine Verbindung mit heruntergefahrenen Koordinationsrechnern herstellen. Die Verbindung wird jedoch wiederhergestellt, wenn die Koordinationsrechner neu gestartet werden.
   - Geplante Prozesse und Operatoren werden während des Aktualisierungsvorgangs nicht ausgeführt.

6. Wenn Sie einen Apache-Lastenausgleich verwenden, kopieren Sie die aktualisierten Apache-Konfigurationsvorlagen von DVD1. Details finden Sie unter Apache-Lastenausgleich (siehe Seite 267).
7. Wenn Sie einen F5-Lastenausgleich verwenden, aktualisieren Sie die iRule-Definition, um die Zuweisung des Primärknotens zu beseitigen. Diese Änderung ermöglicht es Ihnen, in der ersten Phase des Upgrade die veraltete Kommunikation zu weiterverwenden.
   a. Entfernen: set PRIMARY "[PrimaryIP]"
   b. Entfernen: set PRIMPORT "[PrimaryPort]"
   c. Alle Vorkommnisse entfernen: member $PRIMARY $PRIMPORT
8. Stellen Sie sicher, dass auf allen Koordinationsrechner-Knoten eine unterstützte JDK-Version installiert ist. Weitere Informationen finden Sie unter JDK-Voraussetzungen (siehe Seite 79).
9. Wenn der DNS-Hostname, der definiert wurde, als Sie CA Process Automation installiert haben, beschränkte Zeichen enthielt (wie Unterstriche), korrigieren Sie den DNS-Hostnamen. Weitere Informationen finden Sie unter Korrigieren von ungültigen Zeichen im CA Process Automation-DNS-Namen (siehe Seite 254).
10. Stellen Sie sicher, dass CA EEM ausgeführt wird.

    Hinweis: Wenn Sie anstelle von CA Embedded Entitlements Manager (CA EEM) einen LDAP-Server verwendet haben, installieren und starten Sie CA EEM. (CA EEM ist der einzige Verzeichnisserver, der von CA Process Automation 4.0 und höher unterstützt wird.)
11. Führen Sie Upgrades für CA Process Automation-Connectors durch, die nicht der Version 4.x entsprechen.

Durchführen eines Upgrade des Domänen-Koordinationsrechners

Von folgenden CA Process Automation-Versionen können Sie ein direktes Upgrade auf Version 4.2 von CA Process Automation durchführen:

- CA Process Automation Service Pack 3.1sp01
- CA Process Automation Service Pack 4.0sp01
- CA Process Automation Release 4.1
- CA Process Automation Service Pack 4.1sp01

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei dem Host an, auf dem der Domänen-Koordinationsrechner (oder ein Knoten des Domänen-Koordinationsrechners) installiert ist.
2. Navigieren Sie zum Ordner "DVD1" auf dem Installationsdatenträger, und starten Sie den Installationsassistenten über die passende Datei für Ihr Betriebssystem:
   - **Windows:** Domain_Installer_windows.bat
   - **Linux oder UNIX:** Domain_Installer_unix.sh

   Diese Dateien rufen das Drittanbieter-Installationsprogramm und später das Installationsprogramm für den Domänen-Koordinationsrechner auf.
3. Klicken Sie auf "Weiter", um die ersten Seiten des Assistenten zu durchlaufen:
   - Sprache
   - Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation
   - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung
   - Zielverzeichnis auswählen
   - Voraussetzungen für die Installation von CA Process Automation
4. Bei der Installation der JDBC-JAR-Dateien:
   - Wenn Sie Oracle als Datenbankserver verwenden, klicken Sie auf "Weiter".
   - Wenn Sie MySQL oder SQL Server als Datenbankserver verwenden, klicken Sie auf "Dateien hinzufügen".
     - Wenn Sie MySQL verwenden, durchsuchen Sie Ihr System nach dem Speicherort, in den Sie die entsprechende JAR-Datei heruntergeladen haben.
     - Wenn Sie SQL Server verwenden, durchsuchen Sie Ihr System nach ...DVD1\drivers\jtds-1.3.jar.
5. Klicken Sie in "Voraussetzungen für die Installation von CA Process Automation" auf "Weiter".
6. Wenn "Der Setup-Assistent für CA Process Automation wird ausgeführt" angezeigt wird, ersetzen Sie "DVD1" im Verzeichnispfad durch "DVD2". Klicken Sie anschließend auf "Fertig stellen".

   Die folgende Nachricht wird angezeigt: "Das CA Process Automation-Installationsprogramm wird kopiert. Dies kann einige Minuten dauern, bitte warten Sie". Zwischen dem Schließen dieser Seite und dem Öffnen der Seite "Willkommen" kann etwas Zeit vergehen.

7. Wenn "Willkommen beim Setup-Assistenten für CA Process Automation-Domäne" angezeigt wird, klicken Sie sich durch die ersten Seiten des Assistenten:
   - Sprache
   - Willkommen beim Setup-Assistenten für CA Process Automation-Domäne
   - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung
8. Stellen Sie sicher, dass das Java-Startverzeichnis auf die JDK-Version verweist, die von dieser Version unterstützt wird.
9. Fahren Sie fort, sich durch die Seiten zu klicken:
   - Neu installieren
   - Konfigurationsbildschirm
10. Wenn "Zertifikatskennwort festlegen" angezeigt wird, geben Sie das Kennwort ein, das während der Installation der Vorgängerversion angegeben wurde. Notieren Sie das Kennwort für zukünftige Verwendung. Sie werden es benötigen, um Upgrades weiterer Koordinationsrechner und Koordinationsrechner-Knoten in dieser CA Process Automation-Domäne durchzuführen. Klicken Sie auf "Weiter".
11. Klicken Sie sich durch Seite zum Auswählen des Startmenüordners, um Ihre bestehende Auswahl zu verwenden.
12. Beachten Sie auf der Seite "Allgemeine Eigenschaften" die folgenden Änderungen an den Standardwerten für den Koordinationsrechner-Serverport:

    Serverport

    Gibt den Port an, den der Domänen-Koordinationsrechner verwendet, um mit anderen Koordinationsrechnern und Agenten zu kommunizieren. Dieser Port wird für vereinfachte Kommunikation verwendet.

    Standard: 80 (Basis: HTTP) oder 443 (Gesichert: HTTPS)

    Veralteter Serverport

    Der Serverport-Wert, der für eine Vorgängerversion von CA Process Automation definiert war. Dieser Port wird für veraltete Kommunikation verwendet.

    Standard: 7001
13. Klicken Sie sich durch die folgenden Seiten. Nehmen Sie dabei bei Bedarf Änderungen vor.
    - Temporäres Skriptenverzeichnis
    - Richtlinie für PowerShell-Ausführung

14. Wenn die Sicherheitseinstellungen für Embedded Entitlements Manager (EEM) angezeigt werden:
    a. Wählen Sie "Anwendung mit CA EEM registrieren" aus, und klicken Sie auf "Registrieren".
    b. Geben Sie Anmeldeinformationen für die Anmeldung bei CA EEM als EiamAdmin-Administrator an.
    c. Akzeptieren Sie die Durchführung des Upgrade. Der Installationsprozess ermittelt die Version des CA EEM-Servers und wählt den passenden SDK aus.
    d. Wenn die Bestätigung "Anwendung registriert" angezeigt wird, klicken Sie auf "OK".
15. Klicken Sie sich durch die Datenbankeinstellungen, die Sie bereits definiert haben:
    - Repository-Datenbank
    - Laufzeitdatenbank
    - Berichtsdatenbank
16. Wenn nichts hinzugefügt werden muss, klicken Sie sich durch "Zusätzliche JAR-Dateien für Installation".
17. Wenn "Der Setup-Assistent für CA Process Automation-Domäne wird ausgeführt" angezeigt wird, klicken Sie auf "Fertig stellen".

    Wichtig! Es dauert eine Weile, bis der Domänen-Koordinationsrechner für die Anmeldung verfügbar ist. Wenn der Domänen-Koordinationsrechner geclustert ist, kann das Upgrade von zusätzlichen Koordinationsrechnern oder zusätzlichen Knoten erst starten, wenn Sie sich beim Domänen-Koordinationsrechner anmelden können.
18. Starten Sie den Koordinationsrechner-Service auf dem Domänen-Koordinationsrechner.

    Hinweis: Betriebssystemspezifische Details finden Sie unter Starten von Koordinationsrechnern (siehe Seite 143).

Zusätzliche Upgrade-Aufgaben (nach Abschluss des Setup-Assistenten für die Domäne)

1. Ziehen Sie in Erwägung, Werte in *Installationsverzeichnis*/server/c2o/bin/c2osvcw.conf für JVM-Feinabstimmung zu aktualisieren. Zum Beispiel:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Die Werte für "wrapper.java.initmemory" und "wrapper.java.maxmemory" müssen identisch sein. Wenn zusätzlicher Speicher erforderlich und auf dem Server verfügbar ist, können diese Werte geändert werden. Nachdem Sie die Konfigurationswerte geändert haben, starten Sie den CA Process Automation-Service neu.

2. Ziehen Sie in Erwägung, die Standardwerte für JBOSS JMS und Datenbankpools in *Installationsverzeichnis*/server/c2o/conf/standardjboss.xml zu aktualisieren. Zum Beispiel:

   - Unter <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Unter <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

3. Wenn Sie CA EEM 12.51 mit Ihrer aktualisierten CA Process Automation-Installation verwenden und CA EEM für Verweise auf mehrere Microsoft Active Directory-Verzeichnisse oder eine AD-Gesamtstruktur konfiguriert ist, erstellen Sie die CA Process Automation-Anwender in CA EEM neu.

   Hinweis: Siehe "Zugriff für referenzierte Anwenderkonten verwalten" im *Handbuch für Inhaltsadministratoren*.

Weitere Informationen:

Hinweise zu Upgrades (automatische Installation) (siehe Seite 127)

Durchführen eines Upgrade eines nicht geclusterten Koordinationsrechners

Nach einem Upgrade des Domänen-Koordinationsrechners durch Aufrufen eines Skripts, das auf dem Datenträger verfügbar ist, können Sie Upgrades für weitere Koordinationsrechner über die CA Process Automation-Benutzeroberfläche durchführen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Host mit dem Koordinationsrechner, für den das Upgrade durchgeführt werden soll, an.
2. Navigieren Sie zu CA Process Automation, und melden Sie sich mit (siehe Seite 179) Administratoren-Anmeldeinformationen an.
3. Klicken Sie auf die Registerkarte "Konfiguration", und wählen Sie das Auswahlmenü "Installation".
4. Klicken Sie im Abschnitt "Koordinationsrechner installieren" auf "Installieren", um das Upgrade zu starten.
5. Wählen Sie eine Sprache aus, und klicken Sie auf "OK".

   Die Seite "Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation" wird angezeigt.
6. Klicken Sie auf "Weiter", um die folgenden Seiten des Installationsassistenten zu durchlaufen:
   - Lizenzvereinbarung: Wählen Sie die Option zum Akzeptieren der Vereinbarung aus.
   - Standardmäßiges Installationsverzeichnis
   - Voraussetzungen für die Installation von CA Process Automation

7. Führen Sie einen der folgenden Schritte durch, um JDBC JAR-Dateien für die Installation anzugeben:
   - Belassen Sie das Kontrollkästchen "Domäne verwenden" aktiviert, und klicken Sie auf "Weiter". Dadurch wird festgelegt, dass die JDBC-JAR-Dateien verwendet werden, die während der Installation des Domänen-Koordinationsrechners konfiguriert wurden.
   - Schließen Sie den folgenden Vorgang ab:
     a. Deaktivieren Sie das Kontrollkästchen "Domäne verwenden".
     b. Klicken Sie auf "Dateien hinzufügen".
     c. Wählen Sie den Datenbankservertyp aus.
     d. Klicken Sie auf "Durchsuchen", und navigieren Sie zur JDBC JAR-Datei für den ausgewählten Servertypen.
     e. Klicken Sie auf "Weiter".
8. Klicken Sie zum Bestätigen auf "Weiter", und klicken Sie anschließend auf "Fertig stellen", um mit der Ausführung des CA Process Automation-Installationsprogramms fortzufahren.
9. Klicken Sie auf der Seite "Willkommen" auf "Weiter".
10. Aktivieren Sie die Option zum Akzeptieren der Lizenzvereinbarung, und klicken Sie auf "Weiter".
11. Wenn die Seite "Java-Home-Verzeichnis", angezeigt wird, durchsuchen Sie Ihr System nach dem Speicherort des JDK, für den ein Upgrade durchgeführt wurde, und klicken Sie anschließend auf "Weiter".
12. Klicken Sie auf "Weiter", um die folgenden Seiten des Installationsassistenten zu durchlaufen:
    - Domänen-URL
    - Konfigurationsseiten für Single Sign-On und Lastenausgleich
    - Unternehmensname
13. Geben Sie ein Zertifikatskennwort ein, und klicken Sie auf "Weiter".

    Dieses Zertifikatskennwort ist das vom Domänen-Koordinationsrechner verwendete. Tippen Sie dasselbe Zertifikatskennwort ein, das bei der Installation des Domänen-Koordinationsrechners eingegeben wurde. Dabei handelt es sich um dasselbe Zertifikatskennwort, das Sie auch in der Version, von der Sie das Upgrade durchführen, verwendet hatten.

14. Klicken Sie in den folgenden Seiten des Installationsassistenten auf "Weiter", um die bestehende Konfiguration zu akzeptieren:
    - Geben Sie die Einstellungen des Startmenüordners an, und klicken Sie auf "Weiter".
    - Allgemeine Eigenschaften
    - Temporäres Skriptenverzeichnis
    - Richtlinie für PowerShell-Ausführung
    - Einstellungen der Repository-Datenbank für diesen Koordinationsrechner
    - Einstellungen der Laufzeitdatenbank
    - Einstellungen der Berichtsdatenbank
15. Klicken Sie auf "Fertig stellen".
16. Starten Sie den Koordinationsrechner-Service nach Abschluss der Verarbeitung auf dem nicht geclusterten Koordinationsrechner, für den ein Upgrade durchgeführt wurde.

    Hinweis: Betriebssystemspezifische Details finden Sie unter Starten von Koordinationsrechnern (siehe Seite 143).

Zusätzliche Upgrade-Aufgaben

1. Ziehen Sie in Erwägung, Werte in *Installationsverzeichnis*/server/c2o/bin/c2osvcw.conf für JVM-Feinabstimmung zu aktualisieren. Zum Beispiel:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Die Werte für "wrapper.java.initmemory" und "wrapper.java.maxmemory" müssen identisch sein. Wenn zusätzlicher Speicher erforderlich und auf dem Server verfügbar ist, können diese Werte geändert werden.

2. Ziehen Sie in Erwägung, die Standardwerte für JBOSS JMS und Datenbankpools in *Installationsverzeichnis*/server/c2o/conf/standardjboss.xml zu aktualisieren. Zum Beispiel:
   - Unter <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Unter <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

Weitere Informationen:

Beispiel: Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 unter Windows (siehe Seite 299)

Durchführen eines Upgrade eines Cluster-Knoten

Wenn Sie ein Upgrade eines geclusterten Koordinationsrechners durchführen, führen Sie die Upgrades der Knoten einzeln hintereinander durch. Sie können mit einem beliebigen Knoten im Cluster beginnen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei dem Host, auf dem ein Cluster-Knoten installiert ist, an.
2. Navigieren Sie zur URL des Domänen-Koordinationsrechners (bei Clustering der Lastenausgleich für den Domänen-Koordinationsrechner).
3. Melden Sie sich an, klicken Sie auf die Registerkarte "Konfiguration", und klicken Sie anschließend auf das Auswahlmenü "Installation".
4. Klicken Sie unter "Installieren von Cluster-Knoten für Koordinationsrechner" auf "Installieren", um das Upgrade zu starten.
5. Als Erstes wird das Dialogfeld für die Sprachauswahl angezeigt. Klicken Sie auf OK.
6. Klicken Sie sich durch die folgenden Seiten des Assistenten:
   - Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation.
   - Lizenzvereinbarung: Wählen Sie "Ich akzeptiere die Bedingungen der Lizenzvereinbarung" aus
   - Zielverzeichnis auswählen: Standardmäßig C:\Programme\CA\PAM.
   - Voraussetzungen für die Installation von CA Process Automation: Ruft die Installation auf.
   - "Der Setup-Assistent für CA Process Automation wird ausgeführt" (mit "Domäne verwenden" aktiviert): Klicken Sie auf "Fertig stellen"

     Warten Sie, bis die nächste Seite angezeigt wird. Der Fortschritt der Verarbeitung bis zur Anzeige der nächsten Seite wird nicht durch einen visuellen Indikator angezeigt.
   - Willkommen beim Setup-Assistenten für CA Process Automation-Domäne
   - License Agreement (Lizenzvereinbarung)
7. Wenn Sie ein Upgrade Ihres JDK durchgeführt haben, durchsuchen Sie Ihr System nach dem zum Java-Home-Verzeichnis, beispielsweise C:\Programme\Java\jdk1.7.0_45

8. Füllen Sie den Konfigurationsbildschirm aus:
   a. Wenn Sie bereits ein Upgrade für einen Knoten in diesem Cluster durchgeführt haben, wählen Sie in der Drop-down-Liste "Koordinationsrechner" jenen Koordinationsrechner-Knoten aus, für den Sie als Erstes ein Upgrade durchgeführt haben.
   b. Tippen Sie in das Feld "Worker-Knoten für den Lastenausgleich" "node1", "node2", "node3" oder "node4" ein, um den Knoten, für den Sie das Upgrade durchführen, zu identifizieren.
9. Wenn er nicht angezeigt wird, tippen Sie Ihren Unternehmensnamen ein.
10. Geben Sie Ihr Zertifikatskennwort ein.

    Wichtig! Diese Eingabe muss mit dem Zertifikatskennwort übereinstimmen, das beim Upgrade des Domänen-Koordinationsrechners eingegeben wurde.
11. Klicken Sie sich durch die folgenden Seiten, sofern sie angezeigt werden. Die Einstellungen von node1 werden für die weiteren Knoten im Cluster verwendet.
    - Auswahl des Startmenüordners.
    - Seite "Allgemeine Eigenschaften" ("Als Windows-Dienst installieren" wird nicht angezeigt, sondern als Standard verwendet).
    - Temporäres Skriptenverzeichnis
    - PowerShell
    - CA Embedded Entitlements Manager- (CA EEM)-Sicherheitseinstellungen
    - Datenbankeinstellungen - Repository
    - Datenbankeinstellungen - Laufzeit
    - Datenbankeinstellungen - Berichterstellung

    Die Upgrade-Installation wird gestartet.
12. Wenn die Seite "Der Setup-Assistent für CA Process Automation wird ausgeführt" angezeigt wird, klicken Sie auf "Fertig stellen".

    Die Verarbeitung läuft weiter, nachdem Sie auf "Fertig stellen" geklickt haben.
13. Starten Sie den Koordinationsrechner-Service nach Abschluss der Verarbeitung auf dem Cluster-Knoten, für den das Upgrade durchgeführt wurde.

    Hinweis: Betriebssystemspezifische Details finden Sie unter Starten von Koordinationsrechnern (siehe Seite 143).

Zusätzliche Upgrade-Aufgaben

1. Ziehen Sie in Erwägung, Werte in *Installationsverzeichnis*/server/c2o/bin/c2osvcw.conf für JVM-Feinabstimmung zu aktualisieren. Zum Beispiel:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Die Werte für "wrapper.java.initmemory" und "wrapper.java.maxmemory" müssen identisch sein. Wenn zusätzlicher Speicher erforderlich und auf dem Server verfügbar ist, können diese Werte geändert werden.

2. Ziehen Sie in Erwägung, die Standardwerte für JBOSS JMS und Datenbankpools in *Installationsverzeichnis*/server/c2o/conf/standardjboss.xml zu aktualisieren. Zum Beispiel:

   - Unter <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Unter <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

Weitere Informationen:

Beispiel: Upgrade eines Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows (siehe Seite 289)
Beispiel: Upgrade eines weiteren Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows (siehe Seite 296)

Ausführen von Aufgaben nach dem Upgrade

Nachdem Sie ein Upgrade auf Version 4.2 von CA Process Automation durchgeführt haben, schließen Sie folgende Aufgaben nach dem Upgrade ab:

1. Nehmen Sie Änderungen an der Konfigurationsdatei vor.
   a. Navigieren Sie zum folgenden Sicherungsspeicherort:

      `Installationsverzeichnis/config_backup_MM_dd_yyyy_HHmm`

   b. Verwenden Sie ein Tool für Dateienvergleich, um Unterschiede zwischen den Sicherheitskopien und der aktuellen CA Process Automation-Version für folgende Konfigurationsdateien ermitteln.
      `Installationsverzeichnis/server/c2o/.config/OasisConfig.properties`
      `Installationsverzeichnis/server/c2o/bin/c2osvcw.conf`
      `Installationsverzeichnis/server/c2o/conf/standardjboss.xml`
      `Installationsverzeichnis/server/c2o/conf/log4j.xml`

   c. Nehmen Sie an den Dateien der aktuellen CA Process Automation-Version erforderliche Änderungen vor.
2. Navigieren Sie zu CA Process Automation, und melden Sie sich an (siehe Seite 179).
3. Klicken Sie auf die Registerkarte "Konfiguration", und untersuchen Sie den Konfigurationsbrowser.
4. Stellen Sie sicher, dass alle Koordinationsrechner unter dem Koordinationsrechner-Knoten und die zugeordneten Koordinationsrechner-Kontaktpunkte in der Domänenhierarchie in der richtigen Umgebung angezeigt werden. Wenn ein Koordinationsrechner nicht aktiv ist, starten (siehe Seite 143) Sie ihn.
5. Stellen Sie sicher, dass Agenten neu gestartet wurden. Agenten, die veraltete Kommunikation verwenden, werden automatisch neu gestartet. Wenn Agenten heruntergefahren sind, starten Sie sie. Die entsprechende Beschreibung finden Sie unter Starten von Agenten (siehe Seite 190).
6. Wenn Sie CA EEM 12.51 mit Ihrer aktualisierten CA Process Automation-Installation verwenden und Sie CA EEM für Verweise auf mehrere Microsoft Active Directory-Verzeichnisse oder eine AD-Gesamtstruktur konfiguriert haben, legen Sie die Verantwortlichkeit für Objekte neu fest.

   Hinweis: Weitere Informationen finden Sie unter "So ändern Sie die Verantwortlichkeit für ein Automatisierungsobjekt " im *Handbuch für Inhaltsdesign.*

Testen der Prozesse mit den aktualisierten Koordinationsrechnern

Testen Sie Ihre Prozesse nach Abschluss des CA Process Automation-Upgrade. Erwägen Sie folgende Vorgangsweise. Überprüfen Sie, ob die Prozesse auf allen Koordinationsrechnern erfolgreich ausgeführt werden.

Gehen Sie folgendermaßen vor:

1. Starten Sie einen Prozess, der eine Aufgabe generiert. Weisen Sie sich die Aufgabe selbst zu. Überprüfen Sie, ob die Prozessinstanz auf der Registerkarte "Startseite" angezeigt wird. Überprüfen Sie, ob die Aufgabe, die Sie sich zugewiesen haben, in Ihrer Aufgabenliste angezeigt wird.
2. Starten Sie einen geplanten Prozess oder Operator. Überprüfen Sie, ob er pünktlich startet und erfolgreich abschließt.
3. Starten Sie einen Prozess mit Operatoren, die auf Agentenkontaktpunkten oder über Proxy-Kontaktpunkte auf Remote-Hosts ausgeführt werden. Überprüfen Sie, ob die Prozessinstanz erfolgreich abgeschlossen wird.
4. Lassen Sie die Ausführung von Lösungen, die CA Process Automation als eine integrierte Komponente verwenden, zu. Überwachen Sie die Ergebnisse, und überprüfen Sie sie auf unerwartete Vorkommnisse.

Wechseln von Apache- zu NGINX-Lastenausgleich

Wenn Sie vor dem Upgrade für Ihre geclusterten Koordinationsrechner einen Apache-Lastenausgleich verwendet haben, wird empfohlen, diesen Lastenausgleich beizubehalten, bis Sie sichergestellt haben, dass in der neuen Version alles reibungslos funktioniert. Dafür müssen Sie Ihre Apache-Konfiguration mit neuen Vorlagen, die in den Installationsdatenträgern mitgeliefert werden, aktualisieren.

Die Schritte zum Wechseln zu NGINX nach einem Upgrade sind mit der Einrichtung von NGINX in einer neuen Version identisch. Der einzige Unterschied besteht darin, dass Sie NGINX bei einem Upgrade auf demselben Server installieren, auf dem sich der Apache-Lastenausgleich befindet. Dadurch können Sie die bestehende URL und die bestehenden Hostnamen und Ports weiterverwenden.

Details zur Einrichtung finden Sie unter NGINX-Lastenausgleich (siehe Seite 35).

Agenten kommunizieren mit Koordinationsrechnern, und Koordinationsrechner kommunizieren mit Agenten. In Version 4.2 wird eine verbesserte, vereinfachte Kommunikationsmethode eingeführt. Apache verwendet die veraltete Kommunikationsmethode. Standardmäßig werden vorhandene Agenten für die Verwendung der veralteten Kommunikation konfiguriert. Diese Standardeinstellung ermöglicht es Ihnen, nach Abschluss der obligatorischen Upgrade-Aufgaben zu einem günstigen Zeitpunkt von Apache- zu NGINX-Lastenausgleichen zu wechseln und vorhandene Agenten für die Verwendung der vereinfachten Kommunikation zu konvertieren. NGINX unterstützt vereinfachte Kommunikation. (NGINX unterstützt auch veraltete Kommunikation.)

Aktualisieren von F5-Pools, iRule-Definition und Konfiguration

Um vereinfachte Kommunikation zu verwenden, ändern Sie die F5-Konfiguration.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie zwei F5-Pools für jeden CA Process Automation-Cluster (siehe Seite 56).
2. Ersetzen Sie Ihre aktuelle iRule durch die iRule-Definition (siehe Seite 59).
3. Konfigurieren Sie F5, um vereinfachte Kommunikation mit HTTPS zu verwenden (siehe Seite 62).

Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation

Sie müssen vorhandene Agenten neu installieren, um von veralteter Kommunikation zu vereinfachter Kommunikation zu wechseln. Dies kann für alle Agenten durchgeführt werden, nachdem Sie ein Upgrade auf CA Process Automation 04.2.00 durchgeführt und einen NGINX-Lastenausgleich installiert und konfiguriert haben.

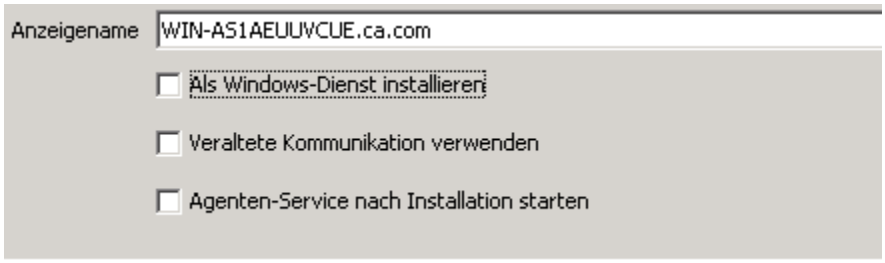
Informationen zum erneuten Installieren der Agenten finden Sie unter Interaktives Installieren eines Agenten (siehe Seite 180). Standardmäßig ist das Kontrollkästchen "Veraltete Kommunikation verwenden" deaktiviert. Wenn dieses Kontrollkästchen deaktiviert bleibt, werden die Agenten für die Verwendung von vereinfachter Kommunikation installiert.

Der Agent erstellt Web-Socket-Verbindungen und sendet die Verbindungsdetails an alle Koordinationsrechner-Knoten. Koordinationsrechner verwenden diese Web-Socket-Verbindung, um bei Bedarf Anfragen oder Aktualisierungen an den Agenten zu senden.

Informationen zur Agent-Kommunikation

Sie konfigurieren Agent-Kommunikationen, wenn Sie einen Agenten installieren. Standardmäßig verwenden neue Agenten vereinfachte Kommunikation (das Kontrollkästchen "Veraltete Kommunikation verwenden" ist deaktiviert).

Agenten, für die ein Upgrade durchgeführt wurde, verwenden veraltete Kommunikation. Sie können diese Einstellung neu konfigurieren, ohne den Agenten neu zu installieren.



Vereinfachte Kommunikation

Die vereinfachte Mitteilung verwendet Web-Sockets und HTTP, um eine einseitige und persistente Verbindung vom Agenten zum Koordinationsrechner herzustellen. CA Process Automation verwendet einen standardmäßigen Port (80 oder 443), der eine schnelle Verbindung zwischen den Komponenten ermöglicht.

Veraltete Kommunikation

Die veraltete Kommunikation mit mehreren Ports kann mit Firewalls und NAT-Routern nicht so gut umgehen wie die vereinfachte Kommunikation. Vom Koordinationsrechner initiierte Verbindungen, die in veralteten Kommunikationsvorgängen verwendet werden, sind weniger effizient als die persistenten Verbindungen, die in vereinfachten Kommunikationsvorgängen verwendet werden.

Weitere Informationen

Vom Lastenausgleich verwendete Ports (siehe Seite 235)

Testen der Prozesse mit vereinfachter Kommunikation

Nachdem Sie den NGINX-Lastenausgleich für alle geclusterten Koordinationsrechner eingerichtet haben, testen Sie Ihre Prozesse erneut. Erwägen Sie folgende Vorgangsweise. Überprüfen Sie, ob die Prozesse auf allen Koordinationsrechnern erfolgreich ausgeführt werden.

Gehen Sie folgendermaßen vor:

1. Starten Sie einen Prozess, der eine Aufgabe generiert. Weisen Sie sich die Aufgabe selbst zu. Überprüfen Sie, ob die Prozessinstanz auf der Registerkarte "Startseite" angezeigt wird. Überprüfen Sie, ob die Aufgabe, die Sie sich zugewiesen haben, in Ihrer Aufgabenliste angezeigt wird.
2. Starten Sie einen geplanten Prozess oder Operator. Überprüfen Sie, ob er pünktlich startet und erfolgreich abschließt.
3. Starten Sie einen Prozess mit Operatoren, die auf Agentenkontaktpunkten oder über Proxy-Kontaktpunkte auf Remote-Hosts ausgeführt werden. Überprüfen Sie, ob die Prozessinstanz erfolgreich abgeschlossen wird.
4. Lassen Sie die Ausführung von Lösungen, die CA Process Automation als eine integrierte Komponente verwenden, zu. Überwachen Sie die Ergebnisse, und überprüfen Sie sie auf unerwartete Vorkommnisse.
5. Wenn Sie sicher sind, dass die neue Version von CA Process Automation, die mit vereinfachter Kommunikation arbeitet, erwartungsgemäß funktioniert, nehmen Sie Ihren normalen Betrieb wieder auf.

Kapitel 7: Neuinstallation oder Konfiguration der aktuellen Version

Sie können Änderungen an der aktuellen Release-Version Ihrer Koordinationsrechner vornehmen, indem Sie den Installationsassistenten wiederholt ausführen. Die Optionen umfassen "Neu installieren" und "Vorhandene Installation konfigurieren".

Dieses Kapitel enthält folgende Themen:

Beispielszenario: Konfigurieren der vorhandenen Installation, um CA Process Automation-Zertifikate neu zu generieren (siehe Seite 168)
Support nach der Installation für CA EEM-Upgrades (siehe Seite 172)
Aktivieren der sicheren Kommunikation für ein vorhandenes CA Process Automation (siehe Seite 176)

Beispielszenario: Konfigurieren der vorhandenen Installation, um CA Process Automation-Zertifikate neu zu generieren

Wenn Sie den Installationsprozess für die zuvor von Ihnen installierte Version ausführen, haben Sie die Möglichkeit, die vorhandene Installation neu zu installieren oder zu konfigurieren. Dieses Beispielszenario zeigt, wie die Option "Vorhandene Installation konfigurieren" verwendet wird, um Zertifikate neu zu generieren, die CA Process Automation verwendet, um eine Verbindung mit CA EEM herzustellen.

Der Installationsprozess des Domänen-Koordinationsrechners ermöglicht es Ihnen, CA Process Automation mit CA EEM zu registrieren (oder neu zu registrieren). Dieser Registrierungsprozess generiert Anwendungszertifikate für CA Process Automation mit der gleichen Schlüssellänge wie die Zertifikate, die CA EEM verwendet.

Hinweis: CA Process Automation hat andere Zertifikate, die nicht von der Registrierung betroffen sind. Die Registrierung generiert nur die Zertifikate, die CA Process Automation verwendet, um eine Verbindung mit CA EEM herzustellen. Der Zertifikatsspeicherort ist "*Installationsverzeichnis*/server/c2o/.c2orepository/public/certification".

Dieses Beispielszenario geht von folgendem Setup aus:

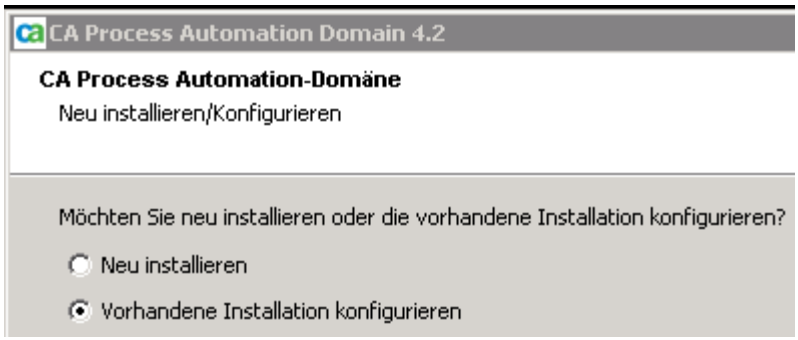
1. Der CA EEM-Administrator verwendet bei der Installation von bzw. dem Upgrade auf Version 12.51 von CA EEM die Standardzertifikate, die 1024-Bit-Schlüssel verwenden.
2. Sie installieren CA Process Automation 4.2 oder führen ein Upgrade auf diese Version durch. Die generierten CA Process Automation-Zertifikate haben auch 1024-Bit-Schlüssel.
3. Später generiert der CA EEM-Administrator neue CA EEM-Zertifikate mit längeren Schlüssellängen (2048-Bit oder 4096-Bit).

Verwenden Sie in diesem Fall den folgenden Vorgang, um CA Process Automation-Zertifikate mit Schlüssellängen, die mit den Schlüssellängen der CA EEM-Zertifikate übereinstimmen, neu zu generieren.

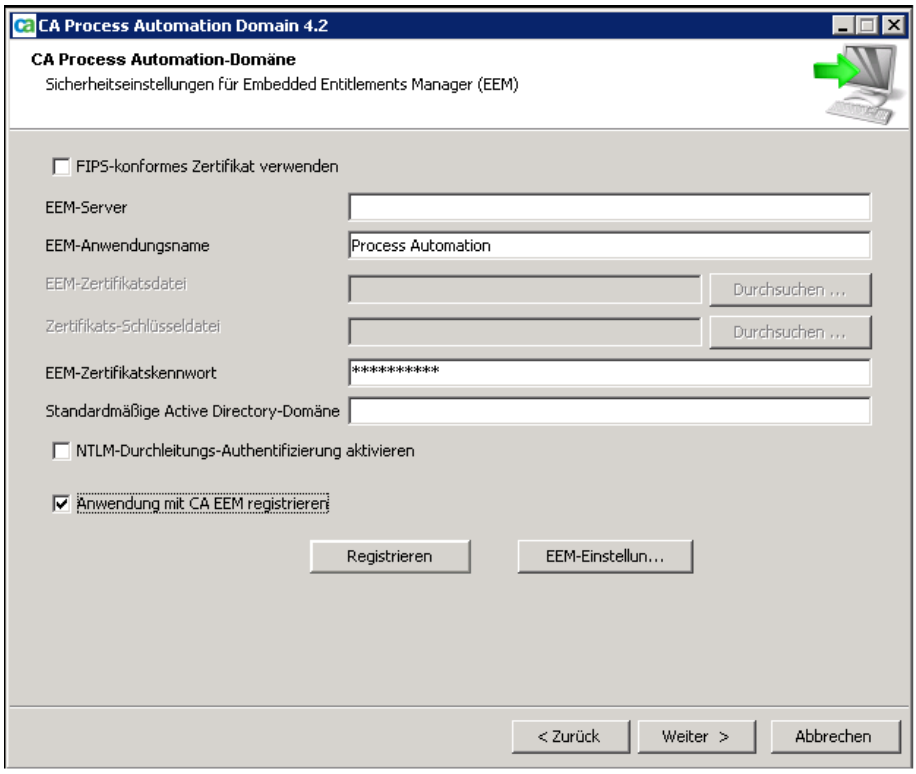
Gehen Sie folgendermaßen vor:

1. Installieren von Drittanbieter-Software (siehe Seite 96).

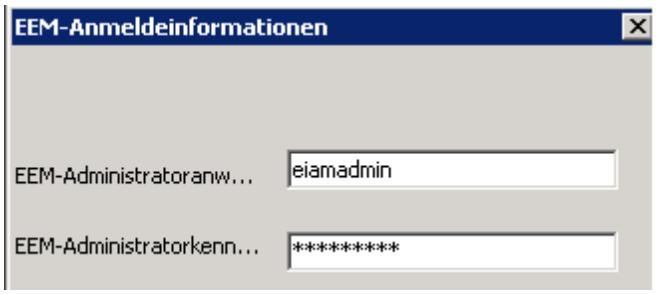
   Wenn die Installation der Drittanbieter-Software fertiggestellt ist, dann wird der Installationsprozess der CA Process Automation-Domänen-Setup gestartet.
2. Klicken Sie durch die ersten Seiten bis die Seite "Neu installieren/Konfigurieren" angezeigt wird.
3. Wählen Sie "Vorhandene Installation konfigurieren". (Dieser Prozess ändert die Eigenschaftsdateien. JAR-Dateien werden nicht geändert.)


CA Process Automation Domain 4.2
CA Process Automation-Domäne
Neu installieren/Konfigurieren
Möchten Sie neu installieren oder die vorhandene Installation konfigurieren?
Neu installieren
Vorhandene Installation konfigurieren

4. Klicken Sie durch die Seiten bis die Seite "Sicherheitseinstellungen für Embedded Entitlements Manager (EEM)" angezeigt wird.
5. Wählen Sie das Kontrollkästchen "Anwendung mit CA EEM registrieren" aus, und klicken Sie dann auf "Registrieren".

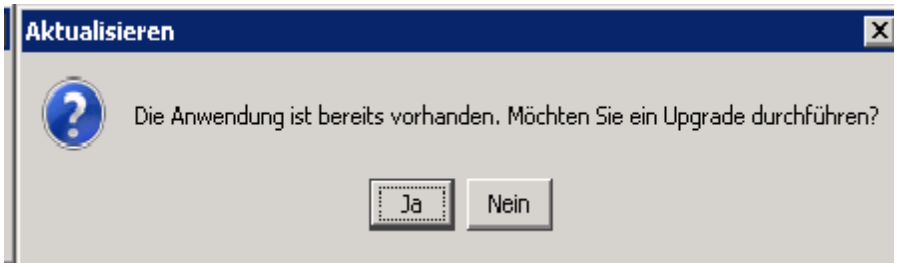


6. Geben Sie die Anmeldeinformationen des CA EEM-Administrators ein. Geben Sie "**EiamAdmin**" für "EEM-Administratoranwendername" ein. Geben Sie das dazugehörige Kennwort ein.



7. Klicken Sie auf "Ja", um ein Upgrade der Anwendung durchzuführen, auch wenn Sie kein Upgrade der CA Process Automation-Version durchführen.

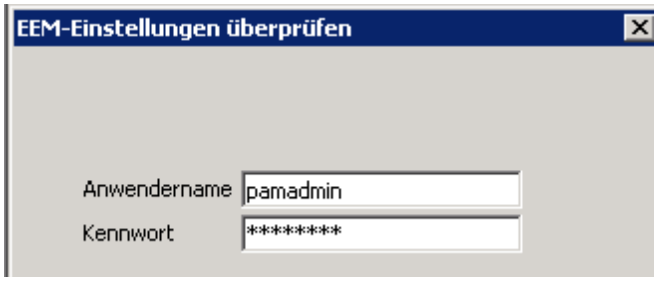
   (Für das Generieren von Anwendungszertifikaten, die CA Process Automation benötigt, ist es erforderlich, dass Sie auf "Ja" klicken.)



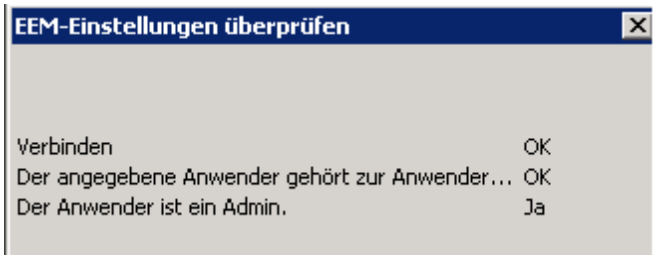
8. Klicken Sie auf "EEM-Einstellungen testen". Klicken Sie bei Setup-Meldungen auf "OK".

9. Geben Sie die Anmeldeinformationen eines CA Process Automation-Anwenders ein, der zur PAMAdmins-Gruppe zugewiesen ist.

   Hinweis: Die Beispieleingabe von **pamadmin**, **pamadmin** ist nur dann gültig, **wenn** Sie CA EEM zur Verwendung des internen Anwenderspeichers konfiguriert haben.



10. Stellen Sie sicher, dass CA Process Automation eine Verbindung mit CA EEM herstellt und dass CA EEM die Anmeldeinformationen authentifiziert.


EEM-Einstellungen überprüfen
Verbinden OK
Der angegebene Anwender gehört zur Anwender... OK
Der Anwender ist ein Admin. Ja

11. Klicken Sie durch den Rest des Installationsprozesses, und klicken Sie dann auf "Fertig stellen".

Support nach der Installation für CA EEM-Upgrades

Wenn Sie den Installationsprozess für dieselbe CA Process Automation-Version ausführen, werden folgende Optionen angezeigt:

Neu installieren

Zeigt den gesamten Installationsassistenten an.

Wählen Sie "Neu installieren" aus, wenn Ihre vorherige Installation den CA EEM-Server mit der Version 8.4 verwendet hat und Sie ein Upgrade des CA EEM-Servers auf Version 12 durchgeführt haben.

- Wenn Sie die Anwendung mit Version 12.x von CA EEM registriert haben, wird bei der Neuinstallation der SDK der Hauptversion, CA EEM 12, ausgewählt.
- Wenn Sie die Anwendung nicht registrieren, werden Sie bei der Neuinstallation dazu aufgefordert, ein SDK basierend auf Ihrer CA EEM-Version auszuwählen.

Wählen Sie "Neu installieren" aus, wenn Sie Version 12.5 von CA EEM verwenden, Ihre SDK-Version jedoch der Hauptversion 8 entspricht. Die Neuinstallation aktualisiert den SDK auf die Hauptversion 12.

Hinweis: CA Process Automation kann die Hauptversion 8 des CA EEM-SDK mit Version 12.x vonCA EEM verwenden. Ein Upgrade des SDK auf Hauptversion 12 ermöglicht es Ihnen, neue CA EEM-Funktionen auszuschöpfen.

Vorhandene Installation konfigurieren

Zeigt nur ausgewählte Seiten an. (Dieser Prozess ändert die Eigenschaftsdateien. JAR-Dateien werden nicht geändert.)

Wählen Sie diese Option aus, wenn Sie CA EEM-Zertifikate mit längeren Schlüsseln (2048 oder 4096) generiert haben, nachdem Sie CA Process Automation 4.2 installiert oder ein Upgrade auf diese Version durchgeführt haben.

Wenn Sie auf der CA EEM-Konfigurationsseite auf "Registrieren" klicken, fordert CA Process Automation Sie dazu auf, ein Upgrade der vorhandenen Anwendung in CA EEM durchzuführen. Wenn Sie dem Upgrade zustimmen, dann werden CA Process Automation-Zertifikate (die für die Kommunikation mit CA EEM verwendet werden) neu generiert. Die neuen CA Process Automation-Zertifikate haben Schlüssellängen, die mit den Längen der CA EEM-Zertifikate übereinstimmen.

Hinweis: Weitere Informationen zum Upgrade von CA EEM oder zum Upgrade der Zertifikate finden Sie in der CA EEM-Dokumentation.

CA Process Automation verwendet das CA EEM-SDK, um mit CA EEM zu kommunizieren. Die Kommunikation ist mit Zertifikaten gesichert. Sowohl CA EEM als auch CA Process Automation haben Zertifikate. CA Process Automation-Zertifikate müssen die gleiche Schlüssellänge wie CA EEM-Zertifikate haben.

Während der Installation von Version 4.2 von CA Process Automation oder dem Upgrade auf Version 4.2 ruft der Installationsprozess die CA Process Automation-Zertifikate aus CA EEM ab und wählt den passenden SDK für die zugeordnete CA EEM-Instanz aus. Diese Zertifikate befinden sich hier:

Installationsverzeichnis/server/c2o/.c2orepository/public/certification

Solange CA EEM nicht geändert wird, ist keine Aktion erforderlich. Allerdings ist Ihr Eingreifen für folgende Änderungen in CA EEM erforderlich.

Installieren Sie Version 4.2 von CA Process Automation mit Version 8.4 von CA EEM, und führen Sie danach ein Upgrade auf Version 12.x von CA EEM durch.

Es ist möglich, keine Aktion auszuführen und trotzdem CA Process Automation mit CA EEM zu verwenden, solange die CA EEM-Zertifikate mit den standardmäßigen Schlüssellängen generiert werden. CA Process Automation kann die Hauptversion 8 des CA EEM-SDK verwenden, um mit Version 12.x von CA EEM zu kommunizieren. Allerdings können Sie mit der Hauptversion 12 des CA EEM-SDK die neuen Funktionen in CA EEM 12.x nutzen.

Wir empfehlen, dass Sie (1) ein Upgrade der Zertifikate durchführen, die CA Process Automation verwendet, um mit CA EEM zu kommunizieren, und dass Sie (2) ein Upgrade von CA Process Automation durchführen, um die Hauptversion 12 des CA EEM-SDK zu verwenden. Führen Sie dazu das Installationsprogramm erneut durch. Folgender Vorgang bezieht sich auf die Schritte in "Installieren des Domänen-Koordinationsrechners (siehe Seite 99)".

- Schritt 5: Wählen Sie "**Neu installieren**" aus (nicht "Vorhandene Installation konfigurieren")
- Schritt 16: Wählen Sie das Kontrollkästchen "**Anwendung mit CA EEM registrieren**" aus.
- Schritt 17: Klicken Sie auf "**Registrieren**", wählen Sie bei der Upgrade-Aufforderung "**Ja**" aus, klicken Sie auf "**OK**", wenn die Bestätigung "Anwendung registriert" angezeigt wird.

Installieren Sie Version 4.2 von CA Process Automation mit Version 12.51 von CA EEM, und generieren Sie anschließend neue CA EEM-Zertifikate mit einer Schlüssellänge von 2048 oder 4096.

1. Version 4.2 von CA Process Automation wird mit Version 12.51 von CA EEM installiert, in welcher Zertifikate mit einer Schlüssellänge von 1024-Bit verwendet werden.
2. Sie generieren neue CA EEM-Zertifikate mit einer Schlüssellänge von 2048 (oder 4096).
3. Sie führen den CA Process Automation-Installationsassistenten erneut aus, wählen diesmal jedoch "Vorhandene Installation konfigurieren" (anstelle von "Neu installieren") aus.
4. Sie registrieren CA Process Automation mit CA EEM. Das bedeutet, den konfigurierten Wert für "EEM-Anwendungsnamen" Wert mit CA EEM zu registrieren. Der Registrierungsprozess generiert neue CA Process Automation-Zertifikate.

Ergebnis: Zertifikate, die CA Process Automation zum Aufrufen von Version 12.51 des CA EEM-SDK verwendet, stimmen mit den längeren Schlüssellängen überein, die von CA EEM verwendet werden.

Weitere Informationen finden Sie unter "Beispielszenario: Konfigurieren der vorhandenen Installation, um CA Process Automation-Zertifikate neu zu generieren (siehe Seite 168)".

Konfigurieren von CA EEM, um es referenzierten Anwendern zu ermöglichen, sich mit einem E-Mail-Namen anzumelden

1. Version 4.2 von CA Process Automation wird mit einer CA EEM-Installation, die einen referenzierten Anwenderspeicher verwendet, installiert. Der referenzierte Anwenderspeicher wird als "Multiple Active Directories" (Mehrere Active Directorys) konfiguriert.
2. Während der CA Process Automation-Installation geben Sie an, welches AD als standardmäßiges Active Directory verwendet werden soll.

   Referenzierte Anwender, die zum standardmäßigen AD gehören, können sich mit ihrem uneingeschränkten Anwendernamen und ihrem Kennwort bei CA Process Automation anmelden.
3. Ohne den nächsten Schritt ermöglicht es CA EEM, dass referenzierte Anwender in anderen Domänen sich mit ihrem Prinzipalnamen (*Domäne\Anwendername*) und Kennwort anmelden.
4. Konfigurieren Sie CA EEM so, dass sich referenzierte Anwender mit ihrem E-Mail-Namen anmelden dürfen (siehe Seite 136).

Ergebnis: Anwender, die sich nicht in der konfigurierten standardmäßigen AD-Domäne befinden, können sich mit ihrem Prinzipalnamen und Ihrem Kennwort anmelden. Für den Prinzipalnamen werden folgende beide Formate unterstützt:

Anwendername@Domäne

Domäne\Anwendername

Übersicht über "Anwendung mit CA EEM registrieren"

- Wenn Sie das Kontrollkästchen "Anwendung mit CA EEM registrieren" aktiviert haben und keine Neuinstallation durchführen, klicken Sie auf **Registrieren**. Sie werden aufgefordert, ein Upgrade der CA Process Automation-Anwendung durchzuführen.
  - Wählen Sie "Ja" aus, um Upgrade auf eine neue Version durchzuführen.
  - Wählen Sie "Ja" aus, um neue CA Process Automation-Zertifikate als Teil des Prozesses "Vorhandene Installation konfigurieren" zu generieren.
  - Wählen Sie "Nein" aus, wenn Sie die gleiche Version neu installieren und keine Zertifikate neu generieren möchten.

Aktivieren der sicheren Kommunikation für ein vorhandenes CA Process Automation

Wenn Sie zuvor "HTTP" als Protokoll ausgewählt haben, über das der Domänen-Koordinationsrechner kommuniziert, können Sie nun beginnen, über das sichere HTTPS-Protokoll zu kommunizieren.

Gehen Sie folgendermaßen vor:

1. Installieren Sie den Domänen-Koordinationsrechner neu. Richten Sie die sichere Kommunikation abhängig von Ihrer Installationsmethode auf eine der folgenden Weisen ein:
   - Wenn Sie den Domänen-Koordinationsrechner interaktiv neu installieren (Installieren des Domänen-Koordinationsrechners (siehe Seite 99)), wählen Sie "Sichere Kommunikation unterstützen" aus.
   - Wenn Sie eine Antwortdatei für eine unbeaufsichtigte Installation des Domänen-Koordinationsrechners erstellen, setzen Sie die Variable "isSecurefest" auf "true", um sichere Kommunikation (HTTPS) zu aktivieren: `isSecure=true`
2. Aktivieren Sie sichere Kommunikation durch Agenten je nach Konfiguration auf eine der folgenden Arten.
   - Stellen Sie sicher, dass Agenten, die für die Verwendung von veralteter Kommunikation konfiguriert sind, automatisch neu gestartet werden. Veraltete Kommunikation ist die Standardeinstellung für vorhandene Agenten, die mit geclusterten Koordinationsrechnern kommunizieren, die einen Apache-Lastenausgleich verwenden. Starten Sie alle Agenten (siehe Seite 190), die heruntergefahren wurden, vor der erneuten Installation.
   - Installieren Sie Agenten, die für die Verwendung von vereinfachter Kommunikation konfiguriert sind, neu. Vereinfachte Kommunikation ist die Standardeinstellung für neue Agenten, die mit geclusterten Koordinationsrechnern kommunizieren, die einen NGINX-Lastenausgleich verwenden. Folgen Sie bei der Neuinstallation von Agenten der Beschreibung unter Installieren eines Agenten (siehe Seite 177). Starten (siehe Seite 190) Sie anschließend die Agenten.

   HTTPS wird für die gesamte Kommunikation zwischen Agenten und Domänen-Koordinationsrechnern verwendet.
3. Stellen Sie auch sicher, dass alle Prozessinstanzen, die vorhandene SOAP-Anhänge verwenden, vollständig sind.

   Hinweis: Auf vorhandene SOAP-Anhänge können Sie nur über HTTP zugreifen.
4. Definieren Sie Firewall-Regeln, um die HTTP-Kommunikationen zu blocken.

Kapitel 8: Installieren von Agenten

Dieses Kapitel enthält folgende Themen:

Voraussetzungen für das Installieren von Agenten (siehe Seite 177)
Navigieren Sie zu CA Process Automation, und melden Sie sich an. (siehe Seite 179)
Interaktives Installieren eines Agenten (siehe Seite 180)
Ausführen einer unbeaufsichtigten Agenteninstallation (siehe Seite 183)
Aufgaben nach der Installation für Agenten (siehe Seite 187)

Voraussetzungen für das Installieren von Agenten

Verwenden Sie folgende Richtlinien zur Vorbereitung der Agenteninstallation:

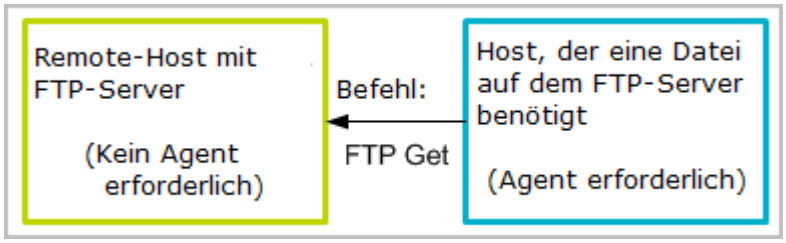
1. Identifizieren von Hosts, die Agenten benötigen (siehe Seite 177).
2. Überprüfen der Java-Voraussetzungen für Agenten (siehe Seite 178).
3. Bestimmen der Portverfügbarkeit für den Agenten (siehe Seite 178) (nur wenn veraltete Kommunikation verwendet wird).

Identifizieren von Hosts, die Agenten benötigen

In den meisten Fällen werden Operatoren auf einem Koordinationsrechner ausgeführt. Das heißt, der Operator verweist auf einen Kontaktpunkt für einen Koordinationsrechner. Operatoren werden auch auf Hosts mit Agenten ausgeführt. In diesem Fall verweist der Operator auf einen Kontaktpunkt, der einem oder mehreren Agenten zugeordnet ist.

Beispiel: Installieren von Agenten auf Hosts, die Operatoren ausführen

Normalerweise installieren Sie CA Process Automation-Agenten auf Hosts, auf denen Operatoren ausgeführt werden, und nicht auf Hosts, mit denen der Operator während der Ausführung eine Verbindung herstellt. Beispiel: Ein Host, der eine Datei auf dem FTP-Server benötigt. Der Host, der die Datei benötigt, führt den Operator "FTP Get" aus. Ein Agent muss auf dem Host installiert sein, auf dem der Operator ausgeführt wird. Auf dem Host mit dem FTP-Server ist kein Agent erforderlich



Hinweis: Wenn es nicht möglich ist, einen Agenten auf einem Remote-Host zu installieren, auf dem ein Operator ausgeführt werden muss, dann können Sie eine SSH-Verbindung von einem Host mit einem Agenten zum Remote-Host erstellen. Weitere Informationen zu Proxy-Kontaktpunkten finden Sie im *Handbuch für Inhaltsadministratoren*.

Überprüfen der Java-Voraussetzungen für Agenten

Bevor Sie einen Agenten auf einem Host installieren, überprüfen Sie, dass die Java-Voraussetzungen erfüllt werden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Host an. Stellen Sie sicher, dass eine unterstützte Version von "Java Runtime Environment JRE" installiert ist. Wenn keine geeignete Version vorhanden ist, laden Sie die JRE vom Anbieter herunter und installieren Sie sie.
2. (Optional) Legen Sie die Umgebungsvariable "JAVA_HOME" auf den Pfad der JRE für den Agenten fest. Wenn diese Variable nicht festgelegt wird, fordert das CA Process Automation-Installationsprogramm Sie auf, zum Verzeichnis zu wechseln, in dem JRE installiert ist.

Bestimmen der Port-Verfügbarkeit für Agenten

Dieser Schritt ist nur für Agenten erforderlich, die veraltete Kommunikation verwenden. Die vereinfachte Kommunikation verwendet Standardports für HTTP (Port 80) und HTTPS (Port 443).

Agenten und Koordinationsrechner kommunizieren über die zwei folgenden Ports miteinander.

- Koordinationsrechner-Port: 7001
- Agenten-Port: 7003

Während der Agenteninstallation konfigurieren Sie die Ports, die Agenten verwenden. Wenn Sie Netzwerkports für einen Agenten konfigurieren, akzeptieren Sie die Standardeinstellungen, außer wenn:

- Eine andere Anwendung auf dem Host den Standardport verwendet.
- Eine Firewall-Beschränkung verhindert die Kommunikation auf dem Standardport.

Um einen Port zu verwenden, der nicht der Standardport ist, wählen Sie einen gültigen und nicht verwendeten Port aus.

Navigieren Sie zu CA Process Automation, und melden Sie sich an.

Die URL, die Sie verwenden, um auf CA Process Automation zuzugreifen, ist davon abhängig, ob der Domänen-Koordinationsrechner mit einem Knoten (nicht-geclustert) oder mit mehreren Knoten konfiguriert (geclustert) ist. Sie können direkt zu einem nicht-geclusterten CA Process Automation navigieren. Navigieren Sie für geclustertes CA Process Automation zum zugeordneten Lastenausgleich. Sie können alle Koordinationsrechner in der Domäne erreichen, indem die URL zum Domänen-Koordinationsrechner oder zum Lastenausgleich für den Domänen-Koordinationsrechner gestartet wird.

Gehen Sie folgendermaßen vor:

1. Durchsuchen Sie CA Process Automation.

   - Verwenden Sie für sichere Kommunikation die folgende Syntax:
     `https://server:port/itpam`

     Beispiele:
     `https://Orchestrator_host:8443/itpam`
     `https://loadBalancer_host:443/itpam`

   - Verwenden Sie für einfache Kommunikation die folgende Syntax:
     `http://server:port/itpam`

     Beispiele:
     `http://Orchestrator_host:8080/itpam`
     `http://loadBalancer_host:80/itpam`

   Die Anmeldeseite von CA Process Automation wird geöffnet.

2. Geben Sie die Anmeldeinformationen von Ihrem Anwenderkonto an.

   Hinweis: Wenn CA EEM so konfiguriert ist, um Anwender von mehreren Microsoft Active Directorys zu referenzieren und CA Process Automation Ihren uneingeschränkten Anwendernamen nicht akzeptiert, geben Sie Ihren Prinzipalnamen ein, d. h. *Domänenname**Anwendername*.

3. Klicken Sie auf Anmelden.

   CA Process Automation wird geöffnet. Die Registerkarte "Startseite" wird angezeigt.

Weitere Informationen

Informationen zur Agent-Kommunikation (siehe Seite 164)

Interaktives Installieren eines Agenten

Prozesse können Operatoren enthalten, die auf Servern mit einer Zielanwendung, einer Datenbank oder einem System ausgeführt werden müssen. Installieren Sie nach Möglichkeit einen Agenten auf solch einem Server. Wenn dies nicht möglich ist, installieren Sie den Agenten auf einem Host, der mit diesem Server über SSH eine Verbindung herstellen kann.

Wichtig! Bevor Sie einen Agenten installieren, stellen Sie sicher, dass der Domänen-Koordinationsrechner ausgeführt wird.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie auf das Auswahlmenü "Installation".
3. Klicken Sie auf "Installieren" für "Agent installieren".

   Es wird ein Dialogfeld angezeigt, das den Fortschritt für das Herunterladen der Anwendung veranschaulicht.
4. Wenn Sie eine Sicherheitswarnung erhalten, klicken Sie auf "Ausführen".

   Das Dialogfeld "Sprachauswahl" wird geöffnet. Die Sprache des Hostcomputers wird standardmäßig ausgewählt.
5. Klicken Sie auf "OK" oder wählen Sie eine andere Sprache aus, und klicken Sie auf "OK".

   Die "Willkommen"-Seite des Setup-Assistenten für den CA Process Automation-Agent wird angezeigt.
6. Klicken Sie auf "Weiter".

   Die Lizenzvereinbarung wird geöffnet.
7. Lesen Sie die Lizenzvereinbarung. Wenn Sie die Bedingungen akzeptieren, klicken Sie auf "Ich akzeptiere die Bedingungen der Lizenzvereinbarung". Klicken Sie auf "Weiter".

   Die Seite "Legen Sie das Java-Home-Verzeichnis fest" wird geöffnet.

8. Wenn das angezeigte Java-Home-Verzeichnis nicht richtig ist, navigieren Sie zum JRE-Ordner.

   Alle Plattformen unterstützen "jre6", Windows unterstützt "jre6" und "jre7".

   Nachfolgend wird ein Beispielpfad für die Windows-Plattform angegeben:

   `C:\Programme\Java\jdk1.7.0_45`

9. Klicken Sie auf "Weiter".

   Die Seite zum Auswählen des Zielverzeichnisses wird geöffnet. Auf Windows-Hosts folgt der Standardpfad:

   `C:\Programme\CA\PAM Agent`

10. Klicken Sie auf "Weiter", um das Standardverzeichnis zu akzeptieren oder geben Sie ein Zielverzeichnis für den neuen Agenten ein, und klicken Sie auf "Weiter".

    Die Seite zum Auswählen des Startmenüordners wird geöffnet.

11. (Nur für Windows) Klicken Sie auf "Weiter", um den CA Process Automation-Agent als Ihre Startmenü-Verknüpfung zu akzeptieren oder geben Sie einen neuen Namen ein, und klicken Sie auf "Weiter".

    - (Optional) Erstellen Sie Verknüpfungen für alle Anwender auf diesem Host.
    - (Optional) Erstellen Sie keinen Startmenüordner.

12. Überprüfen Sie die URL der Domäne. Dabei handelt es sich um die URL, über die Sie die Agenteninstallation gestartet haben. Klicken Sie auf "Weiter".

13. Wenn die Domäne gesichert ist, geben Sie ein Kennwort an.
14. Stellen Sie die Seite "Allgemeine Eigenschaften" fertig, und klicken Sie dann auf "Weiter".
    a. Geben Sie in Agenten-Host den Namen des Agenten-Host ein. Dieser Name identifiziert den Host, von dem Sie die Installation gestartet haben.
    b. Ändern Sie oder akzeptieren Sie den standardmäßigen Anzeigenamen, den Hostnamen.
    c. Wenn Sie die Agenteninstallation von einem Windows-Host gestartet haben, wählen Sie "Als Windows-Dienst installieren" aus.
    d. Um eine neue Verbindung für jede Kommunikation von einem Koordinationsrechner zu einem Agenten zu erzwingen, wählen Sie "Veraltete Kommunikation verwenden" aus.

       Wir empfehlen, dass Sie dieses Kontrollkästchen *deaktivieren*. Vereinfachte Kommunikationen, die Standardeinstellung, wird bevorzugt, weil eine persistente Verbindung verwendet wird.
    e. Wenn Sie "Veraltete Kommunikation verwenden" ausgewählt haben, akzeptieren Sie 7003 als Agentenport, sofern dieser Port nicht verwendet wird. Wenn der Standardport verwendet wird, geben Sie eine nicht verwendete Portnummer wie z. B. 57003 als Port ein, auf dem der Agent die Kommunikation mit Koordinationsrechnern überwacht.

       Hinweis: Wenn die veraltete Kommunikation nicht verwendet wird, dann verwenden Koordinationsrechner eine Web-Socket-Verbindung (von Agenten eingerichtet), um mit Agenten zu kommunizieren. Koordinationsrechner verwenden Port 80, um mit Agenten über HTTP zu kommunizieren. Koordinationsrechner verwenden Port 443, um mit Agenten über HTTPS zu kommunizieren.
    f. Wählen Sie Agenten-Service nach Installation starten aus.

       Das Starten des Agenten ermöglicht es Ihnen, den aktiven Agenten anzuzeigen und mit der Agentenkonfiguration fortzufahren.
15. Klicken Sie auf "Weiter", um das standardmäßige temporäre Verzeichnis für die Ausführung von Skripten zu akzeptieren, oder geben Sie einen anderen Pfad ein, und klicken Sie anschließend auf "Weiter".

    Hinweis: Ein gültiger Pfad enthält keine Leerzeichen.

    Die Seite "PowerShell-Ausführungsrichtlinie festlegen" wird angezeigt.

16. Stellen Sie die Einstellung mit einer der folgenden Methoden fertig.
    - Um Windows PowerShell-Skripte über diesen Agenten auszuführen:
        a. Aktivieren Sie das Kontrollkästchen "PowerShell-Ausführungsrichtlinie festlegen".
        b. Navigieren Sie zum Speicherort des PowerShell-Hosts, wenn dieser vom angezeigten Standard abweicht.
        c. Klicken Sie auf "Weiter".
    - Wenn Sie Windows PowerShell nicht verwenden, klicken Sie auf "Weiter".

    Die Agenteninstallation wird gestartet.
17. Klicken Sie auf "Fertig stellen".
18. (Nur für Windows) Starten Sie den Agenten-Service. Klicken Sie auf "Start", "Programme", "CA", "CA Process Automation-Agent", "Agenten-Service starten".
19. Klicken Sie im Auswahlmenü "Konfigurationsbrowser" auf der Registerkarte "Konfiguration".
20. Klicken Sie auf "Aktualisieren". (Oder: melden Sie sich ab, und melden Sie sich wieder an.)
21. Erweitern Sie "Agenten", und stellen Sie sicher, dass Ihr Agentenname aufgelistet ist.

    Hinweis: Um den Agenten-Host als Ziel zu verwenden, konfigurieren Sie einen Kontaktpunkt. Um den Agenten-Host als Gateway zu einem Remote-Host zu verwenden, konfigurieren Sie einen Proxy-Kontaktpunkt.

Ausführen einer unbeaufsichtigten Agenteninstallation

CA Process Automation unterstützt die unbeaufsichtigte Agenteninstallation, um es Administratoren zu ermöglichen, Agenten remote auf einem Hostcomputer zu installieren. Sie können eine unbeaufsichtigte Installation verwenden, um den Agenten in die anfängliche Konfigurationsroutine für das Einrichten neuer Hostcomputer einzuschließen. Sie können die unbeaufsichtigte Installation auch verwenden, um die Installation durch Software Delivery-Lösungen zu unterstützen.

Wenn Sie die Domänen-URL mit "-VdomainUrl=*domain*_url" eingeben, dann ist *domain_url* http(s):<*FQDN_of_Domain_Orchestrator*>:<*port_number*>.

Wichtig! Die *domain_url* muss ohne **/itpam/** eingegeben werden.

Sie können eine unbeaufsichtigte Agenteninstallation ausführen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
2. Stellen Sie sicher, dass der Domänen-Koordinationsrechner ausgeführt wird.

   Hinweis: Ein unbeaufsichtigtes Agenten-Installationsprogramm muss weiterhin mit dem Domänen-Koordinationsrechner verbunden sein, um erfolgreich einen Agenten zu installieren.
3. Navigieren Sie zum folgenden Verzeichnis:

   `Installationsverzeichnis/server/c2o/.c2orepository/media`

   Der Medienordner enthält die folgenden Dateien:

   - AgentInstaller
   - AgentInstaller.sh
   - AgentInstaller_64
   - AgentInstaller-hpux.sh
   - CA_PAM_Agent_unix.sh
   - CA_PAM_Agent_windows_32
   - CA_PAM_Agent_windows_64
4. Suchen Sie zwei Dateien für Ihr Betriebssystem:
   - Windows (32 Bit): "AgentInstaller.bat" und "CA_PAM_Agent_windows_32.exe"
   - Windows (64 Bit): "AgentInstaller_64.bat" und "CA_PAM_Agent_windows_64.exe"
   - UNIX und Linux: "Agent Install.sh" und "CA_PAM_Agent_unix.sh"
   - HP-UX: "AgentInstaller-hpux.sh" und "CA_PAM_Agent_unix.sh"
5. Kopieren Sie beide Dateien für Ihr Betriebssystem in ein Verzeichnis auf dem Host, auf dem Sie den Agenten installieren möchten.
6. Melden Sie sich bei dem Host an, auf dem Sie den Agenten installieren möchten, und navigieren Sie zum Verzeichnis, in das Sie das Agenten-Installationsprogramm und die Wrapper-Dateien kopiert haben.
7. (Optional) Führen Sie das Agenteninstallationsprogramm ohne Argumente aus, um Hilfe anzuzeigen.
8. Verwenden Sie mit dem Agentinstallationsprogramm folgende Befehlszeilenargumente:

   ```
   AgentInstaller.bat -VdomainUrl=Domänen-URL -VacceptLicense=true
   [-option1 -option2...]
   ```

```
AgentInstaller.sh -VdomainUrl=Domänen-URL
-VacceptLicense=true[-option1 -option2...]
```

Zum Beispiel:

```
-VdomainURL=https://domänenserver.unternehmen.com:8443-VacceptL
icense=true
```

```
-VdomainURL=http://domänenserver.unternehmen.com:8080
```

Das Agenten-Installationsprogramm akzeptiert die folgenden Befehlszeilenoptionen:

–VlisteningAddress=*Hostname*

Gibt den vollqualifizierten Domänennamen oder die IP-Adresse des Hostcomputers an, auf dem Sie den Agenten installieren. Dies wird erforderlich, wenn Ihr Hostcomputer mehrere Netzwerkschnittstellen hat.

-VdisplayName=*display_name*

Gibt den Namen an, der für diesen Agenten angezeigt wird.

-VnodePort=*port_number*

Gibt den auf dem Host zu verwendenden Port an.

-VwinService=*boolean*

Legen Sie den Wert auf "Wahr" fest, um den Agenten als Windows-Service zu installieren.

-Vsys.installationDir=*path*

Gibt den vollständigen Pfad für die Installation auf dem Host an.

-VstartAgent=*boolean*

Legen Sie den Wert auf "Wahr" fest, um den Agenten zu starten, nachdem die Installation abgeschlossen ist.

-VjavaHome=*value*

Gibt den Java-Startspeicherort an.

-Vscripts.tmpDir=*value*

Gibt das temporäre Verzeichnis an, um die Skripten auszuführen.

VcertPassword=*value*

Gibt das Zertifikatskennwort so an, wie es im Domänen-Koordinationsrechner konfiguriert ist. Dieser Wert ist erforderlich, wenn Sie SSL verwenden bzw. im sicheren Modus arbeiten.

VisLookUpDNSForIP=*boolean*

Legen Sie den Wert auf "true" fest, um nach dem Agenten-Hostnamen von DNS zu suchen.

jetty.ssl.ciphers=*value*

Die Liste von durch Kommas getrennten Chiffren, die während der Domänen-Koordinationsrechner-Agentenkommunikation verwendet werden müssen.

-VsetPowerShellExecPolicy=*value*

Die Ausführung von PowerShell-Skripten auf dieser Plattform erfordert, dass die Ausführungsrichtlinie auf "Remote Signed" (per Remote-Zugriff signiert) festgelegt ist. Um PowerShell-Skripten durch CA Process Automation ausführen zu lassen, legen Sie den Wert dieser Variable auf "Wahr" fest.

-VpowerShellPath=*value*

Gibt den PowerShell-Pfad auf einem Hostrechner an.

-VdeprecatedComms=*boolean*

Legt den Kommunikationsmodus (siehe Seite 164) fest. Legen Sie den Wert auf "Wahr" fest, um den veralteten Kommunikationsmodus zu unterstützen. Legen Sie den Wert auf "Falsch" fest, um den neuen Kommunikationsmodus zu unterstützen.

Aufgaben nach der Installation für Agenten

Aufgaben nach der Installation für Agenten sind bedingt.

- Wenn ein Port-Konflikt entsteht, nachdem Sie einen Agenten installiert haben, können Sie Port-Konflikt für den Agenten lösen (siehe Seite 188).
- Wenn Sie Ihr Standort das Ausführen von Agenten mit Root-Berechtigungen nicht erlaubt, können Sie Programme ausführen, um Agenten so zu konfigurieren, dass sie als standardmäßige Anwender mit eingeschränkten Berechtigungen ausgeführt werden (siehe Seite 189).
- Agenten, die mit Version 4.2 von CA Process Automation installiert sind, verwenden standardmäßig die vereinfachte Kommunikation. Im *Handbuch für Inhaltsadministratoren* finden Sie weitere Informationen über das Konfigurieren von Agenten zur Verwendung von veralteter Kommunikation, wenn Sie einen Apache-Lastenausgleich verwenden. Wenn Sie ein Upgrade auf Version 4.2 von CA Process Automation durchgeführt haben, lesen Sie den Abschnitt zur Konfiguration von vorhandenen Agenten für die Verwendung von vereinfachter Kommunikation.

Lösen eines Port-Konflikts für einen Agenten

Wenn ein Port nicht verfügbar ist, nachdem ein Agent installiert wurde, ändern Sie die Port-Zuweisung, indem Sie eine der folgenden Vorgehensweisen verwenden:

- **Windows**:
  1. Navigieren Sie in das folgende Verzeichnis auf dem Host, auf dem der Agent installiert ist:
     `agent_install_dir\.config`
  2. Öffnen Sie die folgende Datei in einem Editor:
     `OasisConfig.properties`
  3. Ändern Sie die folgende Port-Zuweisung:
     `oasis.jxta.port=`
  4. Speichern Sie die Datei. Schließen Sie die Datei.
  5. Navigieren Sie in das folgende Verzeichnis auf dem Server, auf dem der Koordinationsrechner installiert ist.
     `install_dir/server/c2o/.system`
  6. Entfernen Sie den Ordner ".c2o", wenn dieser vorhanden ist.
- **UNIX oder Linux**: Stellen Sie die Boot-Konfiguration ein.

Konfigurieren von Agenten zur Ausführung als standardmäßiger Anwender mit beschränkten Berechtigungen

Die in diesem Abschnitt beschriebenen Programme beziehen sich auf einen Agenten, der auf einem Host mit Windows-Betriebssystem installiert wurde. Diese Programme haben folgende Aufgaben:

- Erstellen Sie das Standardanwenderkonto, das für alle CA Process Automation-Agenten verwendet wird.
- Weisen Sie diesem Agenten auf dem lokalen Host die erforderlichen Rechte zu.

Hinweis: Diese Programme wurden nicht für den Einsatz mit allen Windows-Versionen validiert.

Wenn diese Programme nicht unter Ihrer Windows-Version funktionieren, konfigurieren Sie die Einstellungen manuell. Verwenden Sie den Gruppenrichtlinien-Editor in der Windows-Verwaltung.

Bestimmen Sie, bevor Sie anfangen, das Anwenderkonto *user_name* oder *group_name*, das standardmäßig auf allen installierten Agenten und Koordinationsrechnern verwendet werden soll. Sie können ein normales Anwenderkonto verwenden. Es muss kein Domänenkonto mit Verwaltungsrechten sein.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie eine Eingabeaufforderung. Führen Sie beispielsweise "cmd" aus.
2. Navigieren Sie zum folgenden Verzeichnis:

   `agent_install_dir\PAMAgent\.c2orepository\public\tools`
3. Geben Sie folgenden Befehl ein:

   `itpamsvcacct.bat Anwendername|Gruppenname`

   Das Anwenderkonto wird mit dem Namen erstellt, den Sie festgelegt haben.
4. Geben Sie die folgenden fünf Befehle ein. (Sie können einen einzelnen Befehl eingeben, und ein Leerzeichen als Trennzeichen zwischen Rechten verwenden.)

   `itpamassgnrights.exe user_name host_name + SeTcbPrivilege`

   `itpamassgnrights.exe user_name host_name + SeCreateTokenPrivilege`

   `itpamassgnrights.exe user_name host_name + SeServiceLogonRight`

   `itpamassgnrights.exe user_name host_name + SeBatchLogonRight`

   `itpamassgnrights.exe user_name host_name + SeAssignPrimaryTokenPrivilege`

   Das Anwenderkonto, das Sie angegeben haben, verfügt über die Berechtigungen, die erforderlich sind, um den Agenten auf dem angegebenen lokalen Host auszuführen.

So starten Sie einen Agenten oder halten ihn an:

Die Art und Weise, wie Sie einen Agenten starten und anhalten können, ist vom Betriebssystem abhängig, das auf dem Host verwendet wird, auf dem der Agent installiert ist.

- Starten von Agenten (siehe Seite 190).
- Anhalten von Agenten (siehe Seite 191).

Starten eines Agenten

Verwenden Sie die Methode zum Starten oder erneuten Starten eines Agenten für das Betriebssystem auf dem Host, der den Agenten enthält.

Starten oder erneutes Starten eines Agenten auf einem Microsoft Windows-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem Windows-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows-Host an, auf dem der Agent installiert ist.
2. Wählen Sie im Menü "Start" "Programme", "CA", "CA Process Automation-Agenten", "Agenten-Service starten" aus.
3. Melden Sie sich vom Host ab.

Starten oder erneutes Starten eines Agenten auf einem Linux-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem UNIX- oder Linux-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim UNIX- oder Linux-Host an, auf dem der Agent installiert ist.
2. Nehmen Sie die folgenden Änderungen an Verzeichnissen vor:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Führen Sie folgenden Befehl aus:

   ```
   ./c2oagtd.sh start
   ```

   Der Agent startet neu.

Anhalten von Agenten

Sie können einen CA Process Automation-Agenten anhalten, der auf einem UNIX- oder Linux-Host ausgeführt wird.

Anhalten eines Agenten auf einem Microsoft Windows-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem Windows-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows-Host an, auf dem der Agent installiert ist.
2. Wählen Sie im Menü "Start" "Programme", "CA", "CA Process Automation-Agenten", "Agenten-Service anhalten" aus.
3. Melden Sie sich vom Host ab.

Anhalten eines Agenten auf einem Linux-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem UNIX- oder Linux-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim UNIX- oder Linux-Host an, auf dem der Agent installiert ist.
2. Nehmen Sie die folgenden Änderungen an Verzeichnissen vor:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Führen Sie folgenden Befehl aus:

   ```
   ./c2oagtd.sh stop
   ```

   Der Agent wird angehalten.

Kapitel 9: Hinzufügen eines Knotens zum Domänen-Koordinationsrechner

Sie können die CA Process Automation-Domäne einrichten, indem Sie die Kapazität des Domänen-Koordinationsrechners erweitern. Das Hinzufügen eines Cluster-Knotens hilft dabei, Hochverfügbarkeit für den Domänen-Koordinationsrechner zu erreichen. Folgen Sie für Upgrades von Knoten demselben Prozess, den Sie für das Hinzufügen von Knoten verwendet haben.

Dieses Kapitel enthält folgende Themen:

Voraussetzungen für das Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner (siehe Seite 194)
Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner (siehe Seite 197)
Synchronisieren der Zeit für einen Cluster-Knoten (siehe Seite 199)

Voraussetzungen für das Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner

Sie können einen Cluster-Knoten für den Domänen-Koordinationsrechner installieren. Ein Cluster-Knoten erweitert die Verarbeitungsleistung des Domänen-Koordinationsrechners und kann somit zur Leistungsverbesserung beitragen. Ein Cluster-Knoten nutzt die gleichen Datenbanken, die für die anderen vorhandenen Knoten, die Teil des Clusters des Domänen-Koordinationsrechners sind, konfiguriert wurden.

Bevor Sie die Installation durchführen, führen Sie folgende Voraussetzungen aus:

Gehen Sie folgendermaßen vor:

1. Identifizieren Sie einen Host für den Cluster-Knoten des Koordinationsrechners, der Plattform- und Hardwarevoraussetzungen erfüllt. Weitere Informationen finden Sie in der Komponente "Koordinationsrechner" in den folgenden zwei Themen:
   - Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
   - Hardwareanforderungen (siehe Seite 32).
2. Stellen Sie sicher, dass sich der Host für diesen Cluster-Knoten im gleichen Subnetz wie andere vorhandene Knoten befindet, die Teil des Domänen-Koordinationsrechners sind.
3. Stellen Sie sicher, dass sich der Host für diesen Cluster-Knoten in der gleichen Zeitzone wie andere vorhandene Knoten befindet, die Teil des Domänen-Koordinationsrechners sind.
4. Stellen Sie sicher, dass der Host für diesen Cluster-Knoten ein unterstütztes JDK hat. Wenn das JDK nicht vorhanden ist, laden Sie es herunter.

   Weitere Informationen finden Sie unter JDK-Voraussetzungen (siehe Seite 79).
5. Wenn der Host für diesen Cluster-Knoten eine aktuelle Version von einem Windows-Betriebssystem ausführt, überprüfen Sie die Option "Benutzerkontensteuerung" (unter "Systemsteuerung", "Benutzerkonten"). Wenn diese Option aktiviert ist, deaktivieren Sie das Kontrollkästchen, und starten Sie diesen Server neu.

6. Wenn der Domänen-Koordinationsrechner mit einem F5-Lastenausgleich konfiguriert wurde, fügen Sie dem Lastenausgleich diesen Knoten hinzu.

   Weitere Informationen finden Sie unter Erstellen eines F5-Knoten für jeden Cluster-Knoten (siehe Seite 55).

7. Wenn der Domänen-Koordinationsrechner mit einem Apache-Lastenausgleich konfiguriert wurde, fügen Sie dem Lastenausgleich diesen Knoten hinzu.

   a. Navigieren Sie zu *apache_install_location*\conf.

   b. Öffnen Sie die Datei "workers.properties".

   c. Entfernen Sie die Kommentarzeichen am Anfang der folgenden Zeilen unter "Define Node 2" in der Datei "worker.properties".

      ```
      worker.node2.port=8009
      worker.node2.host=hostname
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Ändern Sie *hostname* in den Hostnamen des Servers, auf dem der Knoten des Domänen-Koordinationsrechners installiert wird.

   e. Fügen Sie "node2" zur Zeile "worker.loadbalancer.balance_workers=" unter dem Lastenausgleichsverhalten hinzu. Die Eingabe ähnelt den folgenden Informationen:

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Hinweis: Befolgen Sie die gleichen Anweisungen für dritte und darauffolgende Knoten, und korrigieren Sie dabei die richtige Knotenzahl für "node2", zum Beispiel "node3" oder "node4".

   f. Starten Sie Apache neu.

8. Wenn der erste Knoten des Domänen-Koordinationsrechners mit einem NGINX-Lastenausgleich konfiguriert wurde, fügen Sie diesen Knoten (node2) dem Lastenausgleich hinzu.

   a. Navigieren Sie zur Datei "pam-server.conf", und öffnen Sie sie.

   b. Suchen Sie die Zeile "#Define node2". (Die node1-Daten beziehen sich auf den ersten Knoten des Domänen-Koordinationsrechners. Überspringen Sie Abschnitte, die sich auf "node1" beziehen)

      Hinweis: "*node2_hostname*" ist die IP-Adresse oder der DNS-Name des Hosts, auf dem "node2" installiert ist. "*jetty_server_port*" ist der Wert "Serverport", der während der Installation des ersten Knotens des Domänen-Koordinationsrechners angegeben wird. Geben Sie 80 für eine vereinfachte Kommunikation ein, oder geben Sie 7003 für eine veraltete Kommunikation ein.

   c. Erstellen Sie folgenden Eingaben in "pam-server.conf", um sowohl "node1" als auch den neuen Knoten "node2" zu definieren:

```
// node1 is the worker node name
upstream node1{
  # Define node1
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
// node2 is the worker node name
upstream node2{
  # Define node2
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

d. Erstellen Sie im Servertag folgende Eingaben sowohl für "node1" als auch für den neuen Knoten "node2":

```
Server{

...
    location = /ws {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node1 {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location /ws/node1/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node2 {
               // node2 is the upstream name provided above
                proxy_pass http://node2;
               }
    location /ws/node2/ {
               // node2 is the upstream name provided above
               proxy_pass http://node2;
               }
}
```

Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner

Anwender mit PAMAdmin-Berechtigungen können einem Domänen-Koordinationsrechner zusätzliche Cluster-Knoten optional hinzufügen. Durch Clustering wird die Verarbeitungslast auf mehrere Hosts, die geclustert werden, verteilt. Clustering ist eine gute Methode, um Hochverfügbarkeit bereitzustellen. Damit der Domänen-Koordinationsrechner für das Clustering geeignet ist, muss ein Lastenausgleich installiert sein, bevor Sie den Domänen-Koordinationsrechner installieren.

Überprüfen Sie den Abschluss der Voraussetzungen für das Installieren eines Cluster-Knotens für den Domänen-Koordinationsrechner (siehe Seite 194). Installieren Sie dann den Cluster-Knoten.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich auf dem Server an, auf dem Sie diesen Cluster-Knoten für den Domänen-Koordinationsrechner installieren möchten.
2. Navigieren Sie zur URL des Domänen-Koordinationsrechners, und melden Sie sich an.

   `https://`*`Lastenausgleichs-Hostname`*`:8443/itpam`

   `http://`*`Lastenausgleichs-Hostname`*`:8080/itpam`
3. Klicken Sie auf die Registerkarte "Konfiguration".
4. Klicken Sie auf das Auswahlmenü "Installation".
5. Klicken Sie auf "Installieren von Cluster-Knoten für Domänen-Koordinationsrechner".
6. Wenn die digitale Signatur nicht überprüft werden kann, klicken Sie auf "Ausführen", um die Installation zu starten.
7. Klicken Sie im Assistenten "Willkommen zum Setup des Installationsprogramms für CA Process Automation-Drittanbieter" auf "Weiter".
8. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".
9. Geben Sie das Zielverzeichnis an, um den Koordinationsrechner-Knoten zu installieren, und klicken Sie auf "Weiter".

   Das Installationsprogramm erstellt den Ordner automatisch, wenn er nicht vorhanden ist.
10. Klicken Sie im Bildschirm "Voraussetzungen für die Installation von CA Process Automation" auf "Weiter".

Die Voraussetzungen in "Der Setup-Assistent für CA Process Automation wird ausgeführt" zeigen das Kontrollkästchen "Domäne verwenden" und einen Pfad an. Stellen Sie sicher, dass dieses Kontrollkästchen ausgewählt ist. Der Installationsprozess verwendet Informationen, die während der Installation des Domänen-Koordinationsrechners erfasst wurden. Dieses Kontrollkästchen wird während Installation normalerweise nicht geändert. Wenn Sie jedoch neue Informationen eingeben müssen, klicken Sie auf das Kontrollkästchen, und geben Sie die neue Informationen ein.

11. Klicken Sie auf "Fertig stellen", um die Installation des Cluster-Knotens für den Domänen-Koordinationsrechner zu starten.
12. Klicken Sie auf dem Begrüßungsbildschirm auf "Weiter".
13. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".
14. Akzeptieren Sie den angezeigten Pfad oder navigieren Sie zum Java-Home-Verzeichnis. Klicken Sie auf "Weiter".

    Das JDK wird validiert, und die Installation des Koordinationsrechners beginnt. Das Kopieren der Konfigurationsdateien wird einen Augenblick dauern.
15. Füllen Sie die Felder auf dem Konfigurationsbildschirm aus, und klicken Sie auf "Weiter".

    Koordinationsrechner

    Gibt den Koordinationsrechner an, zu dem der Cluster-Knoten hinzugefügt werden soll. Der Koordinationsrechner, der in der Drop-down-Liste ausgewählt wird, muss mit einem öffentlichen Hostnamen konfiguriert sein, der den FQDN des Servers angibt, auf dem der Lastenausgleich installiert ist.

    Worker-Knoten für den Lastenausgleich

    Gibt den Knotennamen an, zum Beispiel "node 2". Dies ist der Knotenname, der in der Apache-Datei "workers.properties" angegebenen ist, wobei *hostname* der Name des Hosts ist, auf dem Sie den Cluster-Knoten installieren:

    worker.**node2**.host=*hostname.mycompany*.com

    Hinweis: Die erste Installation des Domänen-Koordinationsrechners ist node1. Geben Sie für den zweiten Knoten **node2** ein.
16. Überprüfen Sie den Unternehmensnamen, und klicken Sie auf "Weiter".
17. Geben Sie das Zertifikatskennwort ein, und klicken Sie auf "Weiter".

    Zertifikatskennwort

    Gibt *dasselbe* Zertifikatskennwort an, das bei der Installation der zuvor installierten Knoten des Domänen-Koordinationsrechners eingegeben wurde.
18. Überprüfen Sie die Einträge in den allgemeinen Eigenschaften für den Koordinationsrechner. Die meisten Einstellungen sind von der Installation des Domänen-Koordinationsrechners abgeleitet. Klicken Sie auf "Weiter".

    Serverhost

Gibt den FQDN des Hosts an, auf dem dieser Cluster-Knoten für den Domänen-Koordinationsrechner installiert ist.

19. Geben Sie einen Startmenüordner an, und klicken Sie auf "Weiter".
20. Zeigen Sie die PowerShell-Einstellungen an.
21. Zeigen Sie die CA EEM-Sicherheitseinstellungen an, und klicken Sie auf "Weiter".
22. Zeigen Sie folgende Datenbankeinstellungen für die Repository-Datenbank (Bibliotheksdatenbank) an, und klicken Sie auf "Weiter".
23. Zeigen Sie folgende Datenbankeinstellungen für die Laufzeitdatenbank an, und klicken Sie auf "Weiter".
24. Zeigen Sie folgende Datenbankeinstellungen für die Berichtsdatenbank an, und klicken Sie auf "Weiter".
25. Sie sollten die Fortschrittsmeldungen überwachen, da das Setup den Cluster-Knoten für den Domänen-Koordinationsrechner auf dem Computer installiert, auf dem Sie die Installation initiiert haben.
26. Klicken Sie auf "Fertig stellen".

    Der Cluster-Knoten für den ausgewählten Domänen-Koordinationsrechner wird installiert.

Synchronisieren der Zeit für einen Cluster-Knoten

Alle Cluster-Knoten für einen Koordinationsrechner müssen die exakt gleiche Uhrzeit haben, die mit einem standardmäßigen externen Zeitserver synchronisiert ist. Entscheiden Sie sich für eine der folgenden Vorgehensweisen, um die Uhrzeit aller Knoten in einem Cluster zu synchronisieren:

- Synchronisieren aller Koordinationsrechner und Cluster-Knoten in einen standardmäßigen externen Zeitserver (bevorzugt).
- Sie können die Zeit aller zusätzlichen Cluster-Knoten folgendermaßen manuell synchronisieren:
  1. Überprüfen Sie die Genauigkeit der Zeit aller Cluster-Knoten.
  2. Führen Sie den entsprechenden BS-Befehl auf jedem Cluster-Knoten aus, um die Zeit aller Cluster-Knoten zu synchronisieren.

Kapitel 10: Installieren von zusätzlichen Koordinationsrechnern

Nach der Installation des Domänen-Koordinationsrechners können Sie die Domäne einrichten, indem Sie zusätzliche Koordinationsrechner installieren. Sie können mehrere Koordinationsrechner in einer Umgebung installieren. Wenn Sie eine neue Umgebung erstellen, zum Beispiel zur Produktionsverwendung, installieren Sie einen Koordinationsrechner in dieser Umgebung.

Dieses Kapitel enthält folgende Themen:

Voraussetzungen für die Installation eines Koordinationsrechners (siehe Seite 201)
Installieren eines Koordinationsrechners (siehe Seite 204)
Aufgaben nach der Installation für den Koordinationsrechner (siehe Seite 210)

Voraussetzungen für die Installation eines Koordinationsrechners

Sie können einen Koordinationsrechner in der Umgebung mit dem Domänen-Koordinationsrechner oder in einer separaten Umgebung installieren. Bevor Sie einen Koordinationsrechner installieren, müssen Sie folgende Voraussetzungen ausführen:

Gehen Sie folgendermaßen vor:

1. Identifizieren Sie einen Host für den Koordinationsrechner, der Plattform- und Hardwarevoraussetzungen erfüllt. Weitere Informationen finden Sie in der Komponente "Koordinationsrechner" in den folgenden zwei Themen:
   - Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
   - Hardwareanforderungen (siehe Seite 32).
2. Stellen Sie sicher, dass der Host für den Koordinationsrechner ein unterstütztes JDK hat. Wenn das JDK nicht vorhanden ist, laden Sie es herunter.

   Weitere Informationen finden Sie unter JDK-Voraussetzungen (siehe Seite 79).

3. Halten Sie das Zertifikatskennwort, das mit dem Schlüsselspeicherkennwort auf dem Domänen-Koordinationsrechner übereinstimmt, bereit. Dieses Kennwort steuert den Zugriff auf die Schlüssel, die zum Verschlüsseln der Kennwörter und anderer kritischer Daten verwendet werden.

   Wichtig! Ohne dieses Kennwort können sie keine weiteren Koordinationsrechner erfolgreich installieren.

4. Identifizieren Sie den Datenbankserver oder die Server, um die Laufzeitdatenbank zu hosten und optional die Repository-Datenbank (Bibliotheksdatenbank) für diesen Koordinationsrechner. Berücksichtigen Sie folgende Faktoren:

   - Jeder Koordinationsrechner muss über eine eigene "Laufzeit"-Datenbank verfügen.
   - Ein Koordinationsrechner kann die Bibliotheksdatenbank des Domänen-Koordinationsrechners gemeinsam nutzen, oder er kann über seine eigene Datenbank verfügen.
   - Normalerweise verwenden alle Koordinationsrechner in der Domäne die Berichtsdatenbank, die für den Domänen-Koordinationsrechner erstellt wurde.
   - Ein Datenbankserver muss die Plattform- und Hardwarevoraussetzungen erfüllen. Weitere Informationen finden Sie in der Komponente "Datenbankserver" in den folgenden zwei Themen:
     - Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
     - Hardwareanforderungen (siehe Seite 32).

5. Bereiten sie den Datenbankserver vor. Die Laufzeit- und Repository-Datenbanken können auf verschiedenen Datenbankservern erstellt werden.

   Weitere Informationen finden Sie unter Datenbankserver-Voraussetzungen (siehe Seite 71).

6. Bewerten Sie den Bedarf eines Lastenausgleichs für diesen Koordinationsrechner. CA Process Automation unterstützt folgende Methoden, um geclusterte Koordinationsrechner auszugleichen.

   Hinweis: Es wird empfohlen, einen hardwarebasierten Lastenausgleich zu verwenden. Weitere Informationen finden Sie unter Voraussetzungen des F5-Lastenausgleichs (siehe Seite 54). Wenn dies nicht möglich ist, wird NGINX als bevorzugter softwarebasierter Lastenausgleich empfohlen. NGINX für UNIX ist hochgradig skalierbar. NGINX für Windows kann bis zu 300 Agenten, die vereinfachte Kommunikation verwenden, unterstützen. Weitere Informationen finden Sie unter Voraussetzungen des NGINX-Lastenausgleichs.

7. Wenn Sie diesen Koordinationsrechner mithilfe von NGINX clustern möchten, nehmen Sie folgende zusätzliche Schritte vor:

   a. Navigieren Sie zur Datei "pam-server.conf", und öffnen Sie sie.

   b. Suchen Sie die Zeile "#Define node1". (Die node1-Daten beziehen sich auf den Koordinationsrechner-Knoten, der als erstes installiert wird.)

   c. Fügen Sie Folgendes ein, wobei "*jetty_server_port*" der Wert ist, der bei der Installation für Serverport konfiguriert ist. Normalerweise sind die Werte für vereinfachte Kommunikation 80 oder 7003, wenn Agenten, die eine Verbindung mit diesem Koordinationsrechner herstellen, veraltete Kommunikation verwenden.

```
// node1 is the worker node name
upstream node1{
  # Define node1
  server node1_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

   d. Erstellen Sie im Servertag folgende Eingaben:

```
Server{
       location = /ws {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/ {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/node1 {
                 // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location /ws/node1/ {
```

```
                    // node1 is the upstream name provided above
                    proxy_pass http://node1;
                    }
...
                    }
}
```

8. Identifizieren Sie einen Zeitserver (NTP-Server). Das Konfigurieren aller Koordinationsrechner zur Verwendung des gleichen externen Zeitservers (oder Ortszeitserver) ist der beste Weg, um Synchronisation sicherzustellen.
9. Stellen Sie sicher, dass Folgendes gestartet ist, bevor Sie zu CA Process Automation navigieren, um die Installation eines Koordinationsrechners zu beginnen:
   - CA EEM.
   - Der Lastenausgleich, wenn dieser verwendet wird.
   - Der Domänen-Koordinationsrechner-Service.
   - Der Datenbankserver, den Sie für die Laufzeitdatenbank verwenden möchten und optional eine separate Repository-Datenbank (oder Bibliotheksdatenbank).

Installieren eines Koordinationsrechners

Nachdem Sie den Domänen-Koordinationsrechner installiert haben, können Sie Koordinationsrechner auf anderen Hosts hinzufügen. Jede neue Umgebung benötigt mindestens einen Koordinationsrechner, jedoch sind mehrere Koordinationsrechner möglich. Mehrere Koordinationsrechner ermöglichen eine Segmentierung. Neue Koordinationsrechner übernehmen die CA EEM-Informationen vom Domänen-Koordinationsrechner.

Bevor Sie den folgenden Vorgang verwenden, schließen Sie die Voraussetzungen für die Installation eines Koordinationsrechners (siehe Seite 201) ab. Stellen Sie zum Beispiel sicher, dass ein JDK installiert ist.

Befolgen Sie den folgenden Prozess, um einen Koordinationsrechner zu installieren oder ein Upgrade eines vorhandenen Koordinationsrechners durchzuführen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei dem Server an, auf dem der neue Koordinationsrechner installiert werden soll.
2. Navigieren Sie zu CA Process Automation, und melden Sie sich mit (siehe Seite 179) Administratoren-Anmeldeinformationen an. Melden Sie sich zum Beispiel als ein Mitglied der Gruppe "PAMAdmins" an.
3. Klicken Sie auf die Registerkarte "Konfiguration", und wählen Sie das Auswahlmenü "Installation".

4. Klicken Sie auf die Verknüpfung der Voraussetzungen, und stellen Sie sicher, dass alle Voraussetzungen erfüllt sind.
5. Klicken Sie auf "Koordinationsrechner installieren".

   Wenn Sie Firefox verwenden, öffnen Sie das Startprogramm von Java (Standard).

   Installieren Sie ggf. das erforderliche Zertifikat nach Anweisung. Die Anwendung wird heruntergeladen. Möglicherweise wird das Dialogfeld zur Sprachauswahl in der Taskleiste angezeigt.
6. Wählen Sie eine Sprache aus, und klicken Sie auf "OK".

   Die Seite "Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation" wird angezeigt.
7. Klicken Sie auf "Weiter".
8. Akzeptieren Sie die Lizenzierungsvereinbarung, und klicken Sie auf "Weiter".
9. Akzeptieren Sie das Standardinstallationsverzeichnis (Installationsverzeichnis) oder ändern Sie es, und klicken Sie auf "Weiter".
10. Klicken Sie auf der Seite "Voraussetzungen für die Installation von CA Process Automation" auf "Weiter".

    Auf der Seite "JBoss wird installiert" wird der Fortschritt der Installation von jboss-5.1 angezeigt.
11. Führen Sie einen der folgenden Schritte durch, um JDBC JAR-Dateien für die Installation anzugeben:
    - Belassen Sie das Kontrollkästchen "Domäne verwenden" aktiviert, und klicken Sie auf "Weiter". Dadurch wird festgelegt, dass die JDBC-JAR-Dateien verwendet werden, die während der Installation des Domänen-Koordinationsrechners konfiguriert wurden.
    - Schließen Sie den folgenden Vorgang ab:
      a. Deaktivieren Sie das Kontrollkästchen "Domäne verwenden".
      b. Klicken Sie auf "Dateien hinzufügen".
      c. Wählen Sie den Datenbankservertyp aus.
      d. Klicken Sie auf "Durchsuchen", und navigieren Sie zur JDBC JAR-Datei für den ausgewählten Servertypen.
      e. Klicken Sie auf "Weiter".
12. Klicken Sie auf dem Bestätigungsbildschirm auf "Weiter".
13. Klicken Sie auf "Fertig stellen", um zum CA Process Automation-Installationsprogramm zu wechseln.
14. Klicken Sie auf dem Begrüßungsbildschirm auf "Weiter".
15. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".

16. Führen Sie auf der Seite "Java-Home-Verzeichnis" eine der folgenden Aktionen aus:
    - Klicken Sie auf "Weiter", um den Standard zu akzeptieren.
    - Durchsuchen Sie das System nach dem JDK-Speicherort, und klicken Sie auf "Weiter".
17. Überprüfen Sie die Domänen-URL, und klicken Sie auf "Weiter".
18. Wenn Sie keinen Lastenausgleich mit Single Sign-on verwenden, klicken Sie auf "Weiter", und überspringen Sie den folgenden Schritt.
19. Füllen Sie diese Seite aus, und klicken Sie auf "Weiter".

    Konfigurieren von Single Sign-on (SSO)

    Gibt an, ob Sie CA SiteMinder mit SSO verwenden. Standardmäßig ist dies deaktiviert. Wenn Sie diese Option auswählen, werden folgende Felder aktiviert:

    - SSO-Authentifizierungstyp (Header)
    - SSO-Authentifizierungsparameter (sm-user)
    - Typ des Servers (Neuer Koordinationsrechner)

    Lastenausgleich konfigurieren

    Gibt an, ob dieser Koordinationsrechner installiert werden soll, sodass er clustern kann.

    Ausgewählt

    Zeigt an, dass ein Lastenausgleich für diesen Koordinationsrechner konfiguriert ist.

    Gelöscht

    Zeigt an, dass kein Lastenausgleich für diesen Koordinationsrechner konfiguriert ist.

    Worker-Knoten (Apache) für den Lastenausgleich

    Gibt den Namen dieses Knotens an. Geben Sie **node1** an, da dieser Koordinationsrechner der erste Knoten in diesem Cluster ist.

    Hinweis: Für Knoten, die nicht node1 entsprechend (beispielsweise node2) siehe:

    - Hinzufügen eines Knotens zum Domänen-Koordinationsrechner (siehe Seite 193).
    - Hinzufügen eines Knotens zu einem zusätzlichen Koordinationsrechner (siehe Seite 211).

Öffentlicher Hostname

Gibt den öffentlichen Hostnamen wie im folgenden Beispiel an:

loadbalancerhost.*mycompany*.com

- Wenn der Domänen-Koordinationsrechner Single Sign-On (SSO) verwendet, gibt dieses Feld den FQDN der IIS- (Internet Information Services) oder der Apache-Anwendung mit dem CA SiteMinder WebAgent an.
- Wenn der Domänen-Koordinationsrechner Single Sign-On (SSO) nicht verwendet, gibt dieses Feld den FQDN des Lastenausgleichs an.

Portnummer des öffentlichen Hosts

Wenn "Sichere Kommunikation unterstützen" deaktiviert ist, gibt dieses Feld den HTTP-Port für den öffentlichen Host an (IIS oder Apache).

Standard

80

Sicherer Port des öffentlichen Hosts

Wenn "Sichere Kommunikation unterstützen" aktiviert ist, gibt dieses Feld den HTTPS-Port für den öffentlichen Host an (IIS oder Apache).

Standard

443

Sichere Kommunikation unterstützen

Gibt an, ob der öffentliche Host HTTPS für die sichere Kommunikation verwendet.

Ausgewählt

Der öffentliche Host verwendet HTTPS für die sichere Kommunikation.

Gelöscht

Der öffentliche Host verwendet HTTPS nicht für die sichere Kommunikation. Stattdessen verwendet er HTTP für die grundlegende Kommunikation.

20. Überprüfen Sie den Unternehmensnamen, und klicken Sie auf "Weiter".
21. Geben Sie das Zertifikatskennwort ein, das der Domänen-Koordinationsrechner verwendet, und klicken Sie auf "Weiter".

    Wenn dieses Zertifikatskennwort verloren geht oder vergessen wird, müssen Sie beginnend mit dem Domänen-Koordinationsrechner alle Koordinationsrechner im CA Process Automation-System neu installieren.

22. Geben Sie die Einstellungen des Startmenüordners an, und klicken Sie auf "Weiter".
23. Geben Sie die allgemeinen Eigenschaften für den Koordinationsrechner ein, und klicken Sie auf "Weiter".

    Serverhost

    Gibt den FQDN dieses Koordinationsrechners an.

    Anzeigename

    Gibt den Namen an, den der Konfigurationsbrowser für diesen Koordinationsrechner anzeigt.

    - Wenn Sie keinen Lastenausgleich konfigurieren, ist der Anzeigename mit dem Serverhostnamen identisch.
    - Wenn Sie einen Lastenausgleich konfigurieren, ist der Anzeigename gleich der FQDN des Servers, der den Lastenausgleich hostet.
24. Akzeptieren Sie die Standardeinstellung, oder legen Sie das temporäre Verzeichnis fest, in dem Skripte ausgeführt werden sollen, klicken Sie dann auf "Weiter".
25. Legen Sie die PowerShell-Ausführungsrichtlinie fest, und klicken Sie auf "Weiter".
26. Führen Sie einen der folgenden Schritte durch, um die Einstellungen der Repository-Datenbank für diesen Koordinationsrechner einzugeben:
    - Schließen Sie den folgenden Vorgang ab, um die vom Domänen-Koordinationsrechner verwendete Repository-Datenbank (Bibliothek) freizugeben:
        a. Geben Sie die gleichen Informationen ein, die Sie für den Domänen-Koordinationsrechner konfiguriert haben.
        b. Klicken Sie auf "Datenbankeinstellungen testen".
        c. Klicken Sie auf "Weiter".
    - Schließen Sie den folgenden Vorgang ab, um eine separate Repository-Datenbank (Bibliothek) für diesen Koordinationsrechner zu erstellen:
        a. Füllen Sie alle Felder aus.
        b. Geben Sie einen eindeutigen Namen für die Repository-Datenbank an.
        c. Klicken Sie auf "Datenbank erstellen".
        d. Klicken Sie auf "Datenbankeinstellungen testen".
        e. Klicken Sie auf "Weiter".

27. Geben Sie die Einstellungen der Laufzeitdatenbank ein. Jeder Koordinationsrechner benötigt eine getrennte Laufzeitdatenbank.
    a. Wenn die neue Laufzeitdatenbank den gleichen Datenbankserver als Repository-Datenbank für diesen Koordinationsrechner verwendet, klicken Sie auf "kopieren aus Haupt-Repository", um den definierten Anwendernamen und das Kennwort zu kopieren.
    b. Wenn der von Ihnen angegebene Datenbankserver der Host für andere Laufzeitdatenbanken ist, erstellen Sie einen gültigen und eindeutigen Namen für diese Laufzeitdatenbank.
    c. Klicken Sie auf "Datenbank erstellen".
    d. Klicken Sie auf "Datenbankeinstellungen testen".
    e. Klicken Sie auf "Weiter".
28. Zeigen Sie "Einstellungen der Berichtsdatenbank" an, und klicken Sie auf "Weiter". Alle Koordinationsrechner in der Domäne nutzen gemeinsam die gleiche Berichtsdatenbank.
29. Klicken Sie auf "Fertig stellen".

Aufgaben nach der Installation für den Koordinationsrechner

Führen Sie nach der Installation folgende Aufgaben nach Bedarf aus.

1. Führen Sie einen der folgenden Schritte durch, um einen Apache-Lastenausgleich zu konfigurieren, um sichere Kommunikation durch SSL zu verwenden:
   a. Wechseln Sie zum folgenden Ordner:
   apache_install_dir\conf\extra\
   b. Öffnen Sie die folgende Datei:
   httpd-ssl.conf
   c. Fügen Sie folgende Zeilen in die Tage <VirtualHost>-</VirtualHost> am Dateiende hinzu:

   ```
   SSLOptions +StdEnvVars +ExportCertData
   JkMount /* loadbalancer
   ```

   Hinweis: Um einen Lastenausgleich für die Verwendung von einfacher Kommunikation zu konfigurieren, sollten die vorherigen Anweisungen mit Kommentarzeichen versehen werden.
   d. Speichern Sie die Datei. Schließen Sie die Datei.
   e. Starten Sie den Apache-HTTP-Server neu.
2. Konfigurieren von Ports (siehe Seite 95).
3. Konfigurieren der Firewalls für bidirektionale Kommunikation (siehe Seite 133).
4. Wenn Sie den Domänen-Koordinationsrechner auf einem Server mit dem Betriebssystem HP-UX installiert haben, führen Sie zusätzliche Konfigurationsschritte auf HP-UX aus.
5. (Nur für Windows) Starten Sie den Koordinationsrechner-Service.

   Der Koordinationsrechner registriert sich am Domänen-Koordinationsrechner.
6. Überprüfen Sie die Installation des zusätzlichen Koordinationsrechners.
   a. Navigieren Sie zu CA Process Automation, und melden Sie sich an.
   b. Klicken Sie auf die Registerkarte "Konfiguration".
   c. Klicken Sie im Auswahlmenü "Konfigurationsbrowser" auf den Knoten "Koordinationsrechner".
   d. Zeigen Sie den neuen Koordinationsrechner in dieser Liste an.

Kapitel 11: Hinzufügen von Knoten zu einem zusätzlichen Koordinationsrechner

Nachdem Sie einen zusätzlichen Koordinationsrechner installiert haben, können Sie dessen Kapazität erweitern und Failover-Funktionen bereitstellen, indem Sie einen Cluster-Knoten hinzufügen. Wenn ein Knoten fehlschlägt, dann übernimmt ein anderer Knoten die Steuerung. Sie können für die Installation von Cluster-Knoten eine interaktive Installation oder eine unbeaufsichtigte Installation verwenden.

Dieses Kapitel enthält folgende Themen:

Voraussetzungen für das Installieren eines Cluster-Knotens für einen Koordinationsrechner (siehe Seite 212)
Installieren von Cluster-Knoten für Koordinationsrechner (siehe Seite 215)
Synchronisieren der Zeit für einen Cluster-Knoten (siehe Seite 217)

Voraussetzungen für das Installieren eines Cluster-Knotens für einen Koordinationsrechner

Sie können einen Cluster-Knoten für einen Domänen-Koordinationsrechner installieren. Ein Cluster-Knoten erweitert die Verarbeitungsleistung eines Domänen-Koordinationsrechners und kann somit zur Leistungsverbesserung beitragen. Ein Cluster-Knoten nutzt die gleichen Datenbanken, die für die anderen vorhandenen Knoten, die Teil des Clusters des Koordinationsrechners sind, konfiguriert wurden.

Führen Sie vor Installation folgenden Voraussetzungen aus:

Gehen Sie folgendermaßen vor:

1. Identifizieren Sie einen Host für den Cluster-Knoten des Koordinationsrechners, der Plattform- und Hardwarevoraussetzungen erfüllt. Weitere Informationen finden Sie in der Komponente "Koordinationsrechner" in den folgenden zwei Themen:
   - Plattformunterstützung und Anforderungen für CA Process Automation-Komponenten (siehe Seite 30).
   - Hardwareanforderungen (siehe Seite 32).
2. Stellen Sie sicher, dass sich der Host für diesen Cluster-Knoten im gleichen Subnetz wie andere vorhandene Knoten befindet, die Teil des Koordinationsrechners sind.
3. Stellen Sie sicher, dass sich der Host für diesen Cluster-Knoten in der gleichen Zeitzone wie andere vorhandene Knoten befindet, die Teil des Koordinationsrechners sind.
4. Stellen Sie sicher, dass der Host für diesen Cluster-Knoten ein unterstütztes JDK hat. Wenn das JDK nicht vorhanden ist, laden Sie es herunter.

   Weitere Informationen finden Sie unter JDK-Voraussetzungen (siehe Seite 79).
5. Wenn der Host für diesen Cluster-Knoten eine aktuelle Version von einem Windows-Betriebssystem ausführt, überprüfen Sie die Option "Benutzerkontensteuerung" (unter "Systemsteuerung", "Benutzerkonten"). Wenn diese Option aktiviert ist, deaktivieren Sie das Kontrollkästchen, und starten Sie diesen Server neu.

6. Wenn der Koordinationsrechner mit einem F5-Lastenausgleich konfiguriert wurde, fügen Sie dem Lastenausgleich diesen Knoten hinzu.

   Weitere Informationen finden Sie unter Erstellen eines F5-Knoten für jeden Cluster-Knoten (siehe Seite 55).

7. Wenn der Koordinationsrechner mit einem Apache-Lastenausgleich konfiguriert wurde, fügen Sie dem Lastenausgleich diesen Knoten hinzu.

   a. Navigieren Sie zu *apache_install_location*\conf.

   b. Öffnen Sie die Datei "workers.properties".

   c. Entfernen Sie die Kommentarzeichen am Anfang der folgenden Zeilen unter "Define Node 2" in der Datei "worker.properties".

      ```
      worker.node2.port=8009
      worker.node2.host=hostname
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Ändern Sie *hostname* in den Hostnamen des Servers, auf dem der Knoten des Koordinationsrechners installiert wird.

   e. Fügen Sie "node2" zu der Zeile "worker.loadbalancer.balance_workers=" unter dem Lastenausgleichsverhalten hinzu. Die Eingabe ähnelt dem folgenden Beispiel:

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Hinweis: Befolgen Sie die gleichen Anweisungen für dritte und darauffolgende Knoten, und korrigieren Sie dabei die richtige Knotenzahl für "node2", zum Beispiel "node3" oder "node4".

   f. Starten Sie Apache neu.

8. Wenn der Koordinationsrechner mit einem NGINX-Lastenausgleich konfiguriert wurde, fügen Sie dem Lastenausgleich diesen Knoten hinzu.

   a. Navigieren Sie zur Datei "pam-server.conf", und öffnen Sie sie.

   b. Suchen Sie die Zeile "#Define node2". (Die node1-Daten beziehen sich auf den ersten Knoten des Koordinationsrechners. Überspringen Sie Abschnitte, die sich auf "node1" beziehen.)

   c. Fügen Sie Folgendes ein

      ```
      # Define node2
        server node2_hostname:jetty_server_port max_fails=3
      fail_timeout=3s;
      }
      ```

      Hinweis: "jetty server port" ist der Wert "Serverport", der während der Installation des ersten Knotens des Domänen-Koordinationsrechners angegeben wurde. Geben Sie 80 für eine vereinfachte Kommunikation ein, oder geben Sie 7003 für eine veraltete Kommunikation ein.

Erstellen Sie im Servertag folgende Eingaben:

```
Server{
     location = /ws {
...
                // node2 is the upstream name provided above
                proxy_pass http://node2;
                }
     location /ws/node2/ {
                // node2 is the upstream name provided above
                proxy_pass http://node2;
                }
}
```

Installieren von Cluster-Knoten für Koordinationsrechner

Anwender mit PAMAdmins-Berechtigungen können zusätzliche Cluster-Knoten an einen Koordinationsrechner, der mit einem Lastenausgleich installiert wurde, hinzufügen.

Überprüfen Sie den Abschluss der Voraussetzungen für das Installieren eines Cluster-Knotens für einen Koordinationsrechner (siehe Seite 212). Installieren Sie dann den Cluster-Knoten. Derselbe Vorgang wird verwendet, um Upgrades von Cluster-Knoten auf eine neue Version durchzuführen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich auf dem Server an, auf dem Sie diesen Cluster-Knoten für den zusätzlichen Koordinationsrechner installieren möchten.
2. Navigieren Sie zum Koordinationsrechner, zu dem Sie den Cluster-Knoten hinzufügen und bei dem Sie sich anmelden möchten.

   `https://`*`Lastenausgleichs-Hostname`*`:8443/itpam`

   `http://`*`Lastenausgleichs-Hostname`*`:8080/itpam`
3. Klicken Sie auf die Registerkarte "Konfiguration", und klicken Sie auf das Auswahlmenü "Installation".
4. Klicken Sie auf "*Installieren von Cluster-Knoten für Koordinationsrechner*".
5. Wenn die digitale Signatur nicht überprüft werden kann, klicken Sie auf "Ausführen", um die Installation zu starten.
6. Klicken Sie im Bildschirm für die Drittanbieterinstallation auf "Weiter".
7. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".
8. Geben Sie das Zielverzeichnis an, um den Koordinationsrechner-Knoten zu installieren, und klicken Sie auf "Weiter".

   Das Installationsprogramm erstellt den Ordner automatisch, wenn er nicht vorhanden ist.
9. Klicken Sie im Bildschirm "Voraussetzungen für die Installation von CA Process Automation" auf "Weiter".

   Der nachfolgende Bildschirm enthält folgende Kontrollkästchen:

   Domäne verwenden

   Gibt an, ob dieser Cluster-Knoten für den Domänen-Koordinationsrechner ist

   Deaktiviert: Gibt an, dass dieser Cluster-Knoten nicht für den Domänen-Koordinationsrechner ist.

   Klicken Sie auf dem Bestätigungsbildschirm auf "Weiter".
10. Klicken Sie auf "Fertig stellen", um zum CA Process Automation-Installationsprogramm zu wechseln.
11. Klicken Sie auf dem Begrüßungsbildschirm auf "Weiter".

12. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf "Weiter".
13. Geben Sie das Java-Home-Verzeichnis an. Im CA Process Automation-Installationsprogramm ist dieses Feld mit dem am besten geeigneten JDK aufgefüllt, das im Pfad gefunden wurde. Wechseln Sie bei Bedarf in das Verzeichnis, in dem JDK installiert wird, und klicken Sie auf "Weiter".

    Das JDK wird validiert, und die Installation des Koordinationsrechners beginnt. Dies wird einen Augenblick dauern, da Dateien kopiert werden.
14. Füllen Sie die Felder auf dem Konfigurationsbildschirm aus, und klicken Sie auf "Weiter".

    Koordinationsrechner

    Gibt den Koordinationsrechner an, zu dem der Cluster-Knoten hinzugefügt werden soll. Der Koordinationsrechner, der in der Drop-down-Liste ausgewählt wird, muss mit einem öffentlichen Hostnamen konfiguriert sein, der den FQDN des Servers angibt, auf dem der Lastenausgleich installiert ist.

    Worker-Knoten für den Lastenausgleich

    Gibt den Knotennamen an, zum Beispiel "node 2". Dies ist der Knotenname, der in der Apache-Datei "workers.properties" angegebenen ist, wobei *hostname* der Name des Hosts ist, auf dem Sie den Cluster-Knoten installieren:

    worker.**node2**.host=*hostname*.*mycompany*.com

    Hinweis: Die erste Installation des Domänen-Koordinationsrechners ist node1. Geben Sie für den zweiten Knoten **node2** ein.
15. Überprüfen Sie den Unternehmensnamen, und klicken Sie auf "Weiter".
16. Geben Sie dasselbe Zertifikatskennwort an, das bei der Installation des Domänen-Koordinationsrechners eingegeben wurde, und klicken Sie auf "Weiter".

    Wenn dieses Zertifikatskennwort verloren geht oder vergessen wird, müssen Sie beginnend mit dem Domänen-Koordinationsrechner alle Koordinationsrechner in Ihrem System neu installieren.
17. Geben Sie einen Startmenüordner an, und klicken Sie auf "Weiter".
18. Geben Sie die allgemeinen Eigenschaften für den Koordinationsrechner ein, und klicken Sie auf "Weiter".

    Weitere Informationen zu den einzelnen Eigenschaften finden Sie unter Installieren und Konfigurieren des Domänen-Koordinationsrechners.
19. Zeigen Sie die Sicherheitseinstellungen an, und klicken Sie auf "Weiter".
20. Zeigen Sie die Datenbankeinstellungen an, und klicken Sie auf "Weiter".
21. Überprüfen Sie die Einstellungen für die Berichtsdatenbank, und klicken Sie auf "Weiter", um die Installation fertig zu stellen.
22. Klicken Sie auf "Fertig stellen".

    Der Cluster-Knoten für den ausgewählten Koordinationsrechner wird installiert.

Synchronisieren der Zeit für einen Cluster-Knoten

Alle Cluster-Knoten für einen Koordinationsrechner müssen die exakt gleiche Uhrzeit haben, die mit einem standardmäßigen externen Zeitserver synchronisiert ist. Entscheiden Sie sich für eine der folgenden Vorgehensweisen, um die Uhrzeit aller Knoten in einem Cluster zu synchronisieren:

- Synchronisieren aller Koordinationsrechner und Cluster-Knoten in einen standardmäßigen externen Zeitserver (bevorzugt).
- Sie können die Zeit aller zusätzlichen Cluster-Knoten folgendermaßen manuell synchronisieren:
  1. Überprüfen Sie die Genauigkeit der Zeit aller Cluster-Knoten.
  2. Führen Sie den entsprechenden BS-Befehl auf jedem Cluster-Knoten aus, um die Zeit aller Cluster-Knoten zu synchronisieren.

Kapitel 12: Feinabstimmung von CA Process Automation

Dieses Kapitel enthält folgende Themen:

So verbessern Sie die Leistung von CA Process Automation (siehe Seite 220)

So verbessern Sie die Leistung von CA Process Automation

Beachten Sie für Ihren Ansatz zur Steigerung oder Verbesserung der Leistung folgende Richtlinien:

- Konvertieren Sie alle eigenständigen Koordinationsrechner in Cluster.

  Das Hinzufügen eines weiteren Knoten kann die Leistung um bis zu 80 % verbessern. Die tatsächlich erzielte Verbesserung hängt von vielen Variablen einschließlich der ausgeführten CA Process Automation-Inhalte ab.

- Inhalt
  - Globale Datensätze

    Verwenden Sie möglichst wenige Verweise auf globale Datensätze, da der Zugriff darauf serialisiert ist. Das bedeutet, dass jeweils nur ein Objekt auf einen Datensatz zugreifen kann. Diese Richtlinie gilt für Schreibvorgänge (nicht für Lesevorgänge).

    Die Best Practice besteht darin, eine Kopie der erforderlichen Daten auf Prozessebene zu erstellen und auf diesen Prozessdatensatz zu verweisen.

  - Inline-Prozesse

    Beschränken Sie das Inline-Starten von Prozessen Reihe auf Fälle, in denen beide folgenden Voraussetzungen zutreffen:

    - Der Inline-Prozess verwendet höchstens 10 Operatoren.
    - Der Inline-Prozess wird nicht in einer Schleife aufgerufen.

- CPUs
  - Überwachen Sie die CPU-Auslastung auf allen Koordinationsrechner-Knoten, um festzustellen, welche Knoten am meisten von zusätzlichen CPUs oder Kernen profitieren könnten.
  - Fügen Sie bei Bedarf weitere CPUs oder Kerne hinzu.
  - Reservieren Sie in virtuellen Umgebungen die CPUs für die VMs von CA Process Automation.

- Arbeitsspeicher
  - Reservieren Sie in virtuellen Umgebungen den RAM für die VMs von CA Process Automation.
  - Überwachen Sie die Auslastung des Prozessspeichers auf allen Koordinationsrechner-Knoten, um festzustellen, ob zusätzlicher RAM benötigt wird.

- Optimierung von VM-Servern

  Konsultieren Sie den Anbieter Ihrer VM-Server für Anweisungen zur Leistungsverbesserung.

- Optimierung und Wartung von Datenbanken

Konsultieren Sie den Anbieter Ihrer Datenbankserver für Anweisungen zum Verbessern und Warten der Leistung der CA Process Automation-Datenbank. Solche Anweisungen umfassen üblicherweise das erneute Indizieren, eine Aktualisierung der Statistik und die Überwachung und Wartung des Dateisystems, in dem Daten gespeichert sind.

- Schalten Sie alle nicht benötigten Funktionen aus.
  - Catalyst

    Wenn Sie keine Catalyst-Connectors verwenden, suchen Sie den folgenden Wert in "OasisConfig.properties", und setzen Sie ihn von "true" auf "false":

    ```
    # enable connector
    ucf.connector.enabled=true
    ```

  - Berichterstellung

    Wenn Sie keine Berichterstellung verwenden, fügen Sie das folgende Schlüssel-Wert-Paar in die Datei "OasisConfig.properties" ein. Änderungen an dieser Datei werden wirksam, wenn der CA Process Automation-Service neu gestartet wird.

    ```
    oasis.disable.reporting.manager=true
    ```

- VMware

  Wenn Sie VMware verwenden, ändern Sie den virtuellen NIC von "E1000" in "VMXNET3" um. Diese Änderung verbessert normalerweise sowohl Leistung als auch Zuverlässigkeit.

Anhang A: So verwenden Sie SiteMinder mit CA Process Automation

CA SiteMinder stellt Single-Sign-On-Fähigkeiten in Domänen mit einzelnen oder mehreren Cookies bereit, sodass Anwender sich nur einmal in jeder Sitzung anmelden müssen, um auf Anwendungen auf verschiedenen Webservern und Plattformen zugreifen zu können.

Dieses Kapitel enthält folgende Themen:

CA SiteMinder-Voraussetzungen (siehe Seite 224)
Konfigurieren der Objekte von CA SiteMinder-Richtlinienservern (siehe Seite 224)
Integrieren von CA Process Automation in IIS für Single Sign-On (siehe Seite 226)
So konfigurieren Sie IIS zur Umleitung an Tomcat (siehe Seite 227)
Integrieren Sie CA Process Automation in Apachen für SSO. (siehe Seite 229)
Aktivieren der Abmeldung in CA Process Automation für SSO (siehe Seite 230)

CA SiteMinder-Voraussetzungen

Stellen Sie sicher, dass Ihr System folgende Voraussetzungen erfüllt, um CA Process Automation mit CA SiteMinder zu installieren:

- Ein mit dem gleichen LDAP/AD integrierter CA EEM-Server wird als Anwenderspeicher auf dem SiteMinder-Richtlinienserver verwendet.
- Ein CA SiteMinder-Webagent, der entweder in IIS oder in Apache integriert ist.

Sie können den Agenten "SiteMinder Apache" nur dann verwenden, wenn ein auf Apache basierter Lastenausgleich und ein geclusterter Koordinationsrechner vorhanden sind. Richten Sie bei einem eigenständigen Koordinationsrechner eine Portweiterleitung von Tomcat 8080 an IIS Port 80 so ein, dass der SM IIS-Agent funktioniert.

Hinweis: Weitere Informationen finden Sie im CA *SiteMinder WebAgent-Installationshandbuch*.

Aus Sicherheitsgründen sollten Sie direkt mit Ihrem CA SiteMinder-Administrator arbeiten, um sicher zu sein, dass Sie die vorhandenen Leitlinien für die Verwendung von CA SiteMinder in Ihrer Organisation verstehen und befolgen.

Wichtig! Sie müssen CA Process Automation-Agenten (nicht nur neu gestartet) neu installieren, wenn sich die URL des Domänen-Koordinationsrechners ändert. Folgende Änderungen können sich auf die URL des Domänen-Koordinationsrechners auswirken:

- Ändern des Domänen-Koordinationsrechners von SSO-aktiviert auf SSO-deaktiviert.
- Ändern des Domänen-Koordinationsrechners von SSO-deaktiviert auf SSO-aktiviert.
- Wechseln des Domänen-Koordinationsrechners zu einem anderen SSO-Server.

Konfigurieren der Objekte von CA SiteMinder-Richtlinienservern

Um CA SiteMinder zu konfigurieren, müssen Sie auf die Verwaltungsoberfläche des CA SiteMinder-Richtlinienservers zugreifen. Weitere Informationen finden Sie im *CA SiteMinder-Richtlinienserver-Konfigurationshandbuch*.

Wichtig! Bevor Sie CA SiteMinder für CA Process Automation konfigurieren, wenden Sie sich an Ihren CA SiteMinder-Administrator. Ihr Unternehmen kann Richtlinien für das Auswählen oder Erstellen von Domänen, Namenskonventionen für andere Entitäten oder andere standortspezifische Sicherheitsbedenke einrichten.

So konfigurieren Sie ein Objekt des Webagenten für die Integration mit CA Process Automation:

1. Erstellen Sie ein Konfigurationsobjekt des Agenten im Infrastrukturbereich der Verwaltungsoberfläche von CA SiteMinder. Wählen Sie entweder "ApacheDefaultSettings" oder "IISDefaultSettings" aus, je nachdem, welchen Webagenten die Webserver hosten werden.
   - Navigieren Sie zur Eigenschaft "BadUrlChars" des Webagenten, und entfernen Sie "/." und "//" aus der Eigenschaft.
   - Navigieren Sie zur Eigenschaft "IgnoreExt", und entfernen Sie den ".gif,.jpg,.jpeg,.png"-Teil des Eigenschaftswerts.
   - Navigieren Sie zur Eigenschaft "LogoffUri", und legen Sie sie auf "/itpam/Logout" fest.
2. Erstellen Sie ein Host-Konfigurationsobjekt. Wählen Sie entweder "ApacheDefaultSettings" oder "IISDefaultSettings" aus, je nachdem, welchen Webagenten die Webserver hosten werden.
3. Erstellen Sie ein Verzeichnisobjekt des Anwenders im Infrastrukturbereich der Verwaltungsoberfläche von CA SiteMinder.
4. Erstellen oder wählen Sie eine Domäne im Domänen-Abschnitt der Verwaltungsoberfläche von CA SiteMinder.
5. Erstellen Sie einen Bereich im Domänen-Abschnitt der Oberfläche des CA SiteMinder-Richtlinienservers.
6. Geben Sie im neuen Bereich den richtigen Agentennamen an, und legen Sie den Ressourcenfilter auf "/itpam" fest. Wählen Sie dann im Abschnitt "Standardressourcenschutz" die Option "Geschützt" aus.
7. Erstellen Sie im neuen Bereich eine Regel mit der Ressource als "*", sodass die Ressource folgendermaßen aussieht: "web_agent/itpam*". Wählen Sie in den Aktionen dann alle aus.

   Hinweis: Geben Sie diese Regel im Abschnitt "Richtlinien" an, indem Sie die Regel zu einer vorhandenen Richtlinie oder zu einer neuen Richtlinie hinzufügen. Weitere Informationen finden Sie im *CA SiteMinder-Richtlinienserver-Konfigurationshandbuch*.
8. Erstellen Sie einen Unterbereich für jede der folgenden URLs, und wählen Sie im Abschnitt "Standardressourcenschutz" die Option "Ungeschützt" aus:
   - /swaref.xsd
   - /genericNoSecurity
   - /images
   - /StartAgent
   - /itpamclient
   - /ServerConfigurationRequestServlet

- /MirroringRequestProcessor
- /soapAttachment
- /AgentConfigurationRequestServlet
- /soap
- /css
- /js

9. Erstellen Sie eine Richtlinie im Abschnitt "Richtlinien", und fügen Sie die Regel hinzu, die Sie in Schritt 7 für Richtlinie erstellt haben.

   Weitere Informationen finden Sie im *CA SiteMinder-Richtlinienserver-Konfigurationshandbuch*.

10. (Optional) Verwenden Sie die Standardwerte, um eine anwenderspezifische Antwortvariable zu erstellen und sie als SSO-Authentifizierungsparameter zu verwenden.

    a. Erstellen Sie ein anwenderdefiniertes Antwortattribut "**pamuser**" vom Typ "WebAgent-HTTP-Header-Variable".

    b. Legen Sie den Variablenwert als Parameter für die Anwender-ID "LDAP-/ActiveDirectory" fest.

    c. Fügen Sie diese anwenderdefinierte Antwort der in Schritt 9 erwähnten Regel hinzu.

       Hinweis: Geben Sie während der CA Process Automation-Installation den Headerparameter "**pamuser**" als SSO-Authentifizierungsparameter mit dem SSO-Authentifizierungstyp als **Header** an. Weitere Informationen finden Sie im *CA SiteMinder-Richtlinienserver-Konfigurationshandbuch*.

Integrieren von CA Process Automation in IIS für Single Sign-On

Hinweis: Um CA SiteMinder mit Clustering zu integrieren, wählen Sie den Apache SiteMinder-Agenten aus.

So konfigurieren Sie Single Sign-On in IIS:

1. Lassen Sie Ihren CA SiteMinder-Administrator CA SiteMinder WebAgent auf einem Computer installieren, auf dem IIS installiert ist.
2. Wenn IIS für SSL konfiguriert wird, entpacken Sie die Datei "IIS_https_httpfolders.zip", die sich im Ordner "/SSO/IIS" des Mediums mit den CA Process Automation-Drittanbieter-Voraussetzungen im Stammverzeichnis der Website befindet, auf der CA SiteMinder integriert wird.

3. Stellen Sie sicher, dass die folgenden Ordner im Stammverzeichnis erstellt sind:
   - c2orepository +
   - itpam
   - mirroringrepository
4. Öffnen Sie IIS-Manager, und entfernen Sie den SSL-Modus aus folgenden Ordnern:

   In der Website:

   - c2orepository
   - mirroringrepository

   Im Ordner "itpam":

   - MirroringRequestProcessor
   - StartAgent
   - genericNoSecurity

   So entfernen Sie den SSL-Modus:

   a. Öffnen Sie die Eigenschaften des entsprechenden Ordners.

   b. Wählen Sie die Registerkarte "Verzeichnissicherheit" aus, klicken Sie im Abschnitt "Sichere Kommunikation" auf die Schaltfläche "Bearbeiten", und deaktivieren Sie das Kontrollkästchen "Sicherer Kanal (SSL) erforderlich".

   Hinweis: Um CA Process Automation zu integrieren, verwenden Sie den Tomcat-Redirector-Filter, wenn der CA SiteMinder-Webagent auf IIS bereitgestellt ist.

So konfigurieren Sie IIS zur Umleitung an Tomcat

Voraussetzungen

Der CA SiteMinder-Agent sollte auf dem gleichen IIS-Server ausgeführt werden, bevor "Tomcat-Redirector" zum Umleiten der Anfragen an CA Process Automation konfiguriert wird. Weitere Informationen finden Sie im *CA SiteMinder-Installationshandbuch*.

Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass der IIS-Webserver installiert und erfolgreich ausgeführt wird.
2. Kopieren Sie den Ordner "TomcatRedirector" auf den Computer, auf dem IIS installiert ist, vorzugsweise unter folgenden Pfad:

   `C:\Programme\CA\SharedComponents`

3. Bearbeiten Sie die Datei "isapi_redirect.properties" im Ordner "bin", um den korrekten Pfad wiederzugeben, wenn ein anderer Pfad angegeben ist.

   Beispiel

   ```
   # Configuration file for the Jakarta ISAPI Redirector
   # The path to the ISAPI Redirector Extension, relative to the
   website
   # This must be in a virtual directory with execute privileges.
   extension_uri=/TomcatRedirector/isapi_redirect.dll
   ```

   Hinweis: TomcatRedirector ist der virtuelle Verzeichnisname.

   ```
   # Full path to the log file for the ISAPI Redirector
   log_file=C:\Program
   Files\CA\SharedComponents\TomcatRedirector\logs\isapi_redirect.
   log
   # Log level (debug, info, warn, error or trace)
   log_level=error
   # Full path to the workers.properties file
   worker_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\workers.propert
   ies
   # Full path to the uriworkermap.properties file\
   worker_mount_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\uriworkermap.pr
   operties
   ```

4. Bearbeiten Sie den Hostnamen in der Datei "TomcatRedirector\conf\workers.properties", um den korrekten Hostnamen wiederzugeben. Ersetzen Sie die Referenzen durch "localhost".

   Beispiel:

   ```
   # statement and uncomment the three worker.ajp13w01 lines
   ##############################################################
   #######
   # The workers that jk should create and work with
   worker.list=ajp13w01
   # Defining a worker named ajp13w01 and of type ajp13
   # Note that the name and the type do not have to match.
   worker.ajp13w01.type=ajp13
   worker.ajp13w01.host=pa-w2k3
   worker.ajp13w01.port=8009
   ```

   Hinweis: Im vorherigen Code ist "pa-w2k3" der Computer, auf dem CA Process Automation installiert ist.

5. Öffnen Sie die IIS-Manager-Konsole.

6. Klicken Sie mit der rechten Maustaste auf die Standard-Webseite, und wählen Sie neues virtuelles Verzeichnis und eine Referenz aus dem Ordner "TomcatRedirector\bin", den Sie unter Schritt 4 erstellt haben.

7. Navigieren Sie im Windows Explorer zum Ordner "TomcatRedirector\logs", und geben Sie alle Berechtigungen der Protokolldatei in diesem Ordner an den Anwender des Netzwerkdienstes.
8. Klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis, wählen Sie "Eigenschaften" aus, klicken Sie neben dem Anwendungsnamen auf "Erstellen", wählen Sie "Scripts and Executables" (Skripte und ausführbare Dateien) für Ausführberechtigungen aus, und klicken Sie auf "OK".

   Hinweis: Stellen Sie sicher, dass der Wert "Anwendungsnamen" und der virtuelle Verzeichnisname, der in der Datei "isapi_redirect.properties" angegeben ist (Schritt 3), identisch sind.

   a. Klicken Sie mit der rechten Maustaste auf "Webdiensterweiterungen", nennen Sie sie "TomcatRedirector", und wählen Sie den Pfad zur Datei "TomcatRedirector\bin\isapi_redirect.dll", um eine Webdiensterweiterung hinzuzufügen. Wählen Sie die Option "Erweiterungsstatus auf 'Zugelassen' setzen" aus.

   b. Wiederverwenden des IIS-Verwaltungsdienstes
9. Fügen Sie "isapi_redirect.dll" als ISAPI-Filter in Ihrer IIS-Website hinzu. Öffnen Sie den IIS-Manager und klicken Sie mit der rechten Maustaste auf den Ordner "Websites", um das Eigenschaftsdialogfeld für alle Websites zu öffnen. Wählen Sie die Registerkarte "ISAPI-Filter" aus, klicken Sie auf "Hinzufügen", und wählen Sie "isapi_redirect.dll" als ausführbare Datei.
10. Stellen Sie sicher, dass Anfragen durch Klicken auf "http://localhost:80" an Tomcat weitergeleitet werden.

Integrieren Sie CA Process Automation in Apachen für SSO.

So konfigurieren Sie Single Sign-On in Apache:

1. Lassen Sie Ihren CA SiteMinder-Administrator CA SiteMinder WebAgent auf einem Computer installieren, auf dem Apache installiert ist.
2. Konfigurieren Sie Apache mit den Einstellungen des öffentlichen Hosts. Weitere Informationen finden Sie unter Installieren des Domänen-Koordinationsrechners (siehe Seite 99).

   Hinweis: Weitere Informationen erhalten Sie von Ihrem CA SiteMinder-Administrator.

Aktivieren der Abmeldung in CA Process Automation für SSO

Sie können eine Single-Sign-On-Abmeldung in CA Process Automation zulassen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zum folgenden Speicherort:

   Installationsverzeichnis/server/c2o/.config

2. Doppelklicken Sie, um die Datei "OasisConfig.properties" zu öffnen.
3. Ändern Sie "ALLOW_SSO_LOGOUT" in "Wahr".

Anhang B: Von CA Process Automation verwendete Ports

Dieser Anhang besteht aus Tabellen, die die Portverwendung der verschiedenen CA Process Automation-Komponenten ausführlich beschreiben. Diese Tabellen sind umfassend und enthalten Duplikate, um für jede Komponente ein vollständiges Bild zur Verfügung zu stellen.

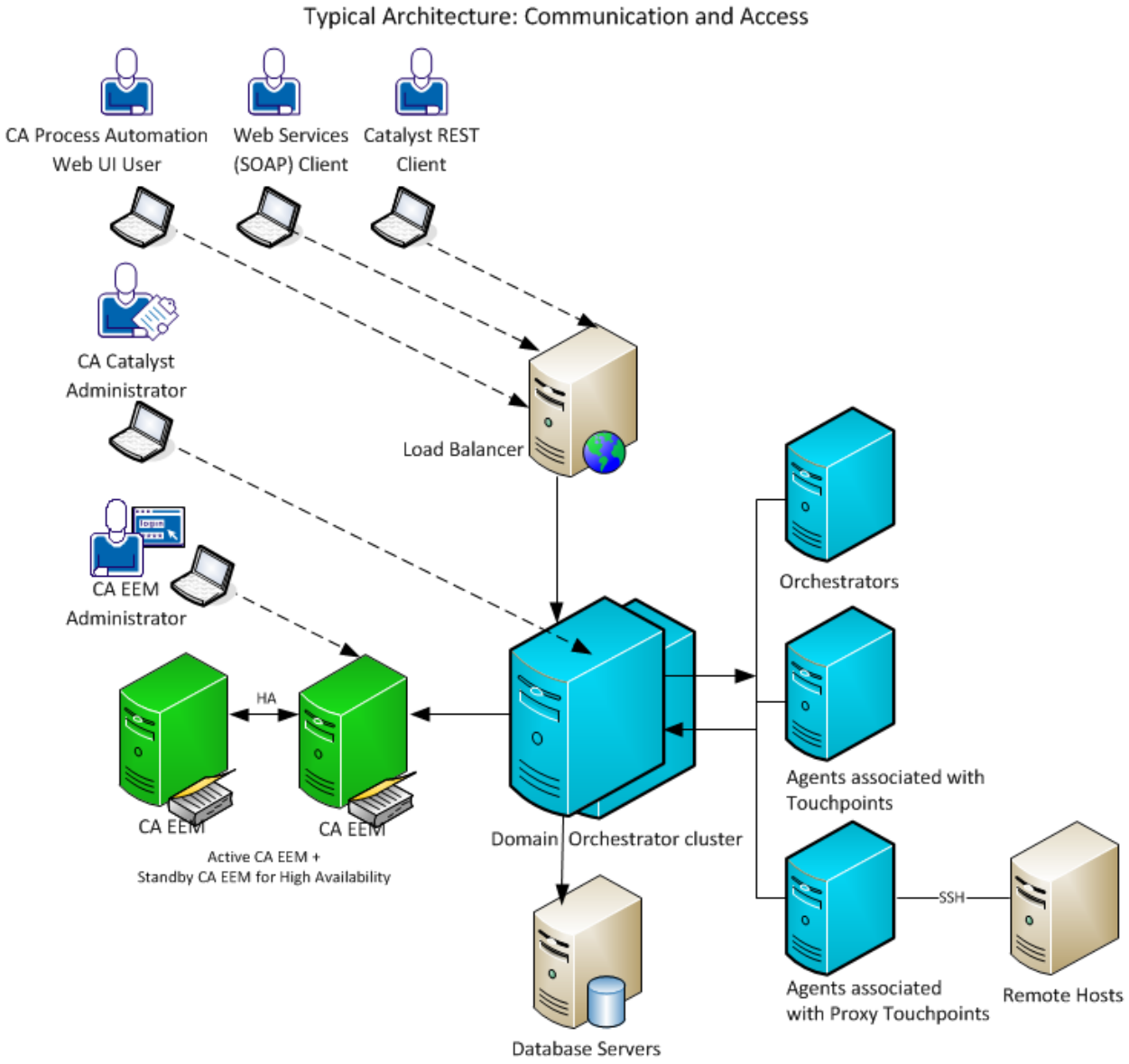
Eine Darstellung der Kommunikation von Komponenten finden Sie in Kommunikation in einer typischen Architektur (siehe Seite 232).

Dieses Kapitel enthält folgende Themen:

Kommunikation in einer typischen Architektur (siehe Seite 232)
Von CA EEM verwendete Ports (siehe Seite 233)
Vom Lastenausgleich verwendete Ports (siehe Seite 235)
Von Koordinationsrechnern verwendete Ports (siehe Seite 238)
Von Agenten verwendete Ports (siehe Seite 249)
Von Datenbankservern verwendete Ports (siehe Seite 250)
Von Web-Clients verwendete Ports (siehe Seite 251)

Kommunikation in einer typischen Architektur

Die folgende Abbildung veranschaulicht die Beziehungen zwischen Komponenten, auf die in diesem Anhang zu von CA Process Automation verwendeten Ports verwiesen wird.



Weitere Informationen:

Planen der Speicherorte für die unterstützenden Komponenten (siehe Seite 69)

Von CA EEM verwendete Ports

Die folgenden Tabellen bieten eine Übersicht über die Ports, die für die Kommunikation von und zu CA Embedded Entitlements Manager (CA EEM) verwendet werden.

Kommunikation von CA EEM

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
CA EEM	Alle	CA EEM	509	TCP	CA EEM-Konfiguration	Von CA EEM iTechPoz verwendet, wenn CA EEM als HA-Cluster konfiguriert ist.
CA EEM	Alle	CA EEM	1684	TCP	CA EEM-Konfiguration	Von CA-EEM iTechPoz Router verwendet, wenn CA EEM als HA-Cluster konfiguriert ist (nur CA EEM 8.4)
CA EEM	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Von CA EEM iGateway verwendet, wenn CA EEM als HA-Cluster konfiguriert ist.

Kommunikation zu CA EEM

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
CA EEM	Alle	CA EEM	509	TCP	CA EEM-Konfiguration	Von CA EEM iTechPoz verwendet, wenn CA EEM als HA-Cluster konfiguriert ist.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
CA EEM	Alle	CA EEM	1684	TCP	CA EEM-Konfiguration	Von CA-EEM iTechPoz Router verwendet, wenn CA EEM als HA-Cluster konfiguriert ist (nur CA EEM 8.4)
CA EEM	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Von CA EEM iGateway verwendet, wenn CA EEM als HA-Cluster konfiguriert ist.
Koordinationsrechner	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Von CA EEM iGateway verwendete Ports
Webbrowser (CA EEM-Administrator)	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Webbrowser, der auf die CA EEM-Benutzeroberfläche zugreift.

Vom Lastenausgleich verwendete Ports

Die folgende Tabellen bieten eine Übersicht über Ports, die für Kommunikation vom und zum konfigurierten Lastenausgleich verwendet werden. Unterstützte Lastenausgleiche umfassen NGINX, Apache und F5. Ports umfassen Lastenausgleiche für "Jboss@Koordinationsrechner" und "Jetty@Koordinationsrechner".

Kommunikation vom Lastenausgleich

Hinweis: Listener-Ports für einen Lastenausgleich können in der Datei, die in der Spalte "Konfiguration" angegeben ist, konfiguriert werden. Die Dokumentation der einzelnen Lastenausgleiche beschreibt den Speicherort der jeweiligen Konfigurationsdatei.

Apache

httpd.conf

tomcat.connector.ajp.port

NGINX

pam-server.conf

secure-pam-server.conf

pam-rest.conf

F5

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Lastenausgleich	Alle	Koordinationsrechner	80	HTTP	httpd.conf	Der Lastenausgleich kommuniziert mit dem Koordinationsrechner auf diesem Port. Dieser Port gilt nicht für NGINX.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Lastenausgleich	Alle	Koordinationsrechner	443	HTTPS	httpd.conf	Der Lastenausgleich kommuniziert mit sicheren Koordinationsrechnern auf diesem Port. Dieser Port gilt nicht für NGINX.
Lastenausgleich	Alle	Koordinationsrechner	8010	TCP/AJP	tomcat.connector.ajp.port	Lastenausgleich: AJP-Connector-Port zwischen Lastenausgleich und Koordinationsrechner. Dieser Port gilt nicht für NGINX.
Lastenausgleich	Alle	Koordinationsrechner	8080	HTTP	httpd.conf, pam-server.conf	Der Lastenausgleich kommuniziert mit dem Koordinationsrechner auf diesem Port.
Lastenausgleich	Alle	Koordinationsrechner	8443	HTTPS	httpd.conf, secure-pam-server.conf	Der Lastenausgleich kommuniziert mit sicheren Koordinationsrechnern auf diesem Port.
Lastenausgleich	Alle	Koordinationsrechner	8009	TCP/AJP	tomcat.connector.ajp.port	Lastenausgleich: AJP-Connector-Port zwischen Lastenausgleich und Koordinationsrechner. Dieser Port gilt nicht für NGINX.
Lastenausgleich	Alle	Koordinationsrechner	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Port des CA Process Automation-Catalyst-Container
Lastenausgleich	Alle	Koordinationsrechner	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Sicherer Port des CA Process Automation-Catalyst-Container

Kommunikation zum Lastenausgleich

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Catalyst-REST-Client	Alle	Lastenausgleich	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Port des CA Process Automation-Catalyst-Container
Catalyst-REST-Client	Alle	Lastenausgleich	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Sicherer Port des CA Process Automation-Catalyst-Container
Agent	Alle	Lastenausgleich	80	HTTP	httpd.conf	Port des Lastenausgleichs für einfache Kommunikation
Agent	Alle	Lastenausgleich	443	HTTPS	httpd.conf	Port des Lastenausgleichs für sichere Kommunikation
Webbrowser (CA Process Automation-Anwender)	Alle	Lastenausgleich	80	TCP	httpd.conf	Port des Lastenausgleichs für einfache Kommunikation
Webbrowser (CA Process Automation-Anwender)	Alle	Lastenausgleich	443	TCP	httpd.conf	Port des Lastenausgleichs für sichere Kommunikation
Webservice-Client (SOAP)	Alle	Lastenausgleich	80	TCP	httpd.conf	Port des Lastenausgleichs für einfache Kommunikation
Webservice-Client (SOAP)	Alle	Lastenausgleich	443	TCP	httpd.conf	Port des Lastenausgleichs für sichere Kommunikation

Von Koordinationsrechnern verwendete Ports

Die folgenden Tabellen bieten eine Übersicht über die Ports, die für folgende Arten der Kommunikation verwendet werden:

- Kommunikation von einem Koordinationsrechner zu einer anderen Komponente in einem CA Process Automation-System
- Kommunikation zwischen Koordinationsrechnern
- Kommunikation zu einem Koordinationsrechner von einer anderen Komponente in einem CA Process Automation-System

Kommunikation von einem Koordinationsrechner zu einer anderen Komponente

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Von CA EEM iGateway verwendete Ports
Koordinationsrechner	Alle	Agent	7003	HTTP/ HTTPS	Skript für Agenteninstallation	**Veraltet** Agent überwacht diesen veralteten Port, wenn der alte Kommunikationsmodus mit Koordinationsrechnern verwendet wird
Koordinationsrechner	Alle	Microsoft SQL-Datenbankserver	1433	TCP	In Microsoft SQL konfiguriert	Der Datenbankport kann in der Installation des Datenbankservers geändert werden. Der Standardwert ist 1433.
Koordinationsrechner	Alle	MySQL-Datenbankserver	3306	TCP	In MySQL konfiguriert	Der Datenbankport kann in der Installation des Datenbankservers geändert werden. Der Standardwert ist 3306.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Oracle-Datenbankserver	1521	TCP	In Oracle konfigurierter Listener	Der Datenbankport kann im Schritt "Create Listener" geändert werden. Der Standardwert für den Oracle Listener-Port ist 1521. Die Datenbankinstanz kann zu einem anderen Listener zugeordnet werden. Konsultieren Sie die Oracle-Konfiguration.
Koordinationsrechner	Alle	Ziel-Remote-Host	22	TCP	Standardmäßiger SSH-Port	Für SSH-Kommunikation mit einem Proxy-Kontaktpunkt oder einer Hostgruppe verwendet

Kommunikation zwischen Domänen-Koordinationsrechnern und Nicht-Domänen-Koordinationsrechnern

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Domänen-Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1090	TCP	jboss.remoting.port	Der Port für JBoss Remoting wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1098	TCP	jboss.rmi.port	Der Port für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1099	TCP	jboss.jndi.port	Der Port für JBoss JNDI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1100	TCP	jboss.ha.jndi.port	JBoss: Die HA-Java Naming and Directory Interface-Schnittstelle wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1101	TCP	jboss.ha.jndi.port	JBoss: HA-Java Remote Method Invocation wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	1102	UDP	jboss.mcast.jndi.autodiscovery.port	JBoss: JNDI Autodiscovery wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	3873	TCP	jboss.remoting.transport.Connector.port	JBoss: EJB3 Remoting Connector wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4444	TCP	jboss.rmi.object.port	Der Serverport für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	Der Port für JBoss Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4446	TCP	jboss.pooledinvoker.serverbind.port	Der Port für JBoss HA Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4447	TCP	jboss.ha.rmi.object.port	Der Serverport für JBoss HA-RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4448	TCP		Der Port für JBoss HA Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4457	TCP	jboss.service.binding.port	Der Port für JBoss Messaging wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4712	TCP	jboss.tx.recovery.manager.port	Der Port für JBoss Transaction Status Recovery Manager wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	4713	TCP		Der Port für JBoss Transaction Status Manager wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	7001	HTTP/ HTTPS	oasis.jxta.port	Für Kommunikation zwischen Koordinationsrechnern verwendeter Port.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	7600	TCP	jboss.jgroups.tcp.tcp_port	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	7900	TCP	jboss.messaging.datachanneltcpport	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	7901	TCP	jboss.messaging.controlchanneltcpport	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	8083	TCP	jboss.rmi.classloader.webservice.port	Der WebService-Port für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	8080			
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner	8443			
Koordinationsrechner	Alle	Nicht-Domänen-Koordinationsrechner				

Kommunikation zwischen geclusterten Koordinationsrechner-Knoten

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Koordinationsrechner	1090	TCP	jboss.remoting.port	Der Port für JBoss Remoting wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	1098	TCP	jboss.rmi.port	Der Port für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	1099	TCP	jboss.jndi.port	Der Port für JBoss JNDI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Koordinationsrechner	1100	TCP	jboss.ha.jndi.port	JBoss: Die HA-Java Naming and Directory Interface-Schnittstelle wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	1101	TCP	jboss.ha.jndi.port	JBoss: HA-Java Remote Method Invocation wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	1102	UDP	jboss.mcast.jndi.autodiscovery.port	JBoss: JNDI Autodiscovery wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	3873	TCP	jboss.remoting.transport.Connector.port	JBoss: EJB3 Remoting Connector wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4444	TCP	jboss.rmi.object.port	Der Serverport für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	Der Port für JBoss Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Koordinationsrechner	4446	TCP	jboss.pooledinvoker.serverbind.port	Der Port für JBoss HA Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4447	TCP	jboss.ha.rmi.object.port	Der Serverport für JBoss HA-RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4448	TCP		Der Port für JBoss HA Pooled Invoker wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4457	TCP	jboss.service.binding.port	Der Port für JBoss Messaging wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4712	TCP	jboss.tx.recovery.manager.port	Der Port für JBoss Transaction Status Recovery Manager wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	4713	TCP		Der Port für JBoss Transaction Status Manager wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Koordinationsrechner	7001	HTTP/ HTTPS	oasis.jxta.port	Für Kommunikation zwischen Koordinationsrechnern verwendeter Port.
Koordinationsrechner	Alle	Koordinationsrechner	7600	TCP	jboss.jgroups.tcp.tcp_port	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	7900	TCP	jboss.messaging.datachanneltcpport	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	7901	TCP	jboss.messaging.controlchanneltcpport	Der Port für JBoss-Clustering wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	8083	TCP	jboss.rmi.classloader.webservice.port	Der WebService-Port für JBoss RMI wird nur für die Kommunikation zwischen Koordinationsrechnern verwendet.
Koordinationsrechner	Alle	Koordinationsrechner	61618			ActiveMQ...

Hinweis: CA Process Automation verwendet JBoss 5.1. Wenn JBoss 5.1 als ein Cluster für die Kommunikation zwischen Knoten (nur Koordinationsrechner) konfiguriert ist, werden intervallweise dynamische Ports im Bereich 49152-65535 verwendet. Viele Ports werden für Verwaltungsvorgänge innerhalb des Cluster verwendet. CA empfiehlt, Cluster zwischen WAN-Links und Firewalls nicht zu teilen. Der Standardkonfiguration für Cluster verwendet Multicast. Wenn Multicast-Kommunikation zwischen Cluster-Knoten nicht durchgehend geöffnet ist, gehören sie nicht zum selben Cluster, was zu unvorhersagbarem Verhalten führen kann.

Kommunikation zu einem geclusterten Koordinationsrechner von einer anderen Komponente

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Lastenausgleich	Alle	Koordinationsrechner	8080	HTTP	Apache httpd.conf	Der Apache-Lastenausgleich kommuniziert mit Koordinationsrechnern auf diesem Port.
Lastenausgleich	Alle	Koordinationsrechner	8443	HTTPS	Apache httpd.conf	Der Apache-Lastenausgleich kommuniziert mit sicheren Koordinationsrechnern auf diesem Port.
Lastenausgleich	Alle	Koordinationsrechner	7000	HTTP	node0-config.xml, http.port	Port des CA Process Automation-Catalyst-Container
Lastenausgleich	Alle	Koordinationsrechner	7443	HTTPS	node0-config.xml, https.port	Sicherer Port des CA Process Automation-Catalyst-Container
Lastenausgleich	Alle	Koordinationsrechner	8009	TCP/AJP	tomcat.connector.ajp.port	Lastenausgleich: AJP-Connector-Port zwischen Lastenausgleich und Koordinationsrechner
Agent	Alle	Koordinationsrechner	8080	HTTP	tomcat.connector.http.port	Nur veraltete Kommunikation.
Agent	Alle	Koordinationsrechner	8443	HTTPS	tomcat.secure.port	Nur veraltete Kommunikation.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Agent	Alle	Koordinationsrechner	7001	HTTP/ HTTPS	oasis.jxta.port	Veralteter Port

Kommunikation zu einem nicht geclusterten Koordinationsrechner von einer anderen Komponente

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Agent	Alle	Koordinationsrechner	8080	HTTP	tomcat.connector.http.port	CA Process Automation-Benutzeroberfläche - Basis-Port
Agent	Alle	Koordinationsrechner	8443	HTTPS	tomcat.secure.port	CA Process Automation-Benutzeroberfläche - Sicherer Port
Agent	Alle	Koordinationsrechner	7001	HTTP/ HTTPS	oasis.jxta.port	Veralteter Port
Koordinationsrechner	Alle	Agent	80	HTTP	Jetty	Web-Socket-Verbindung, die von Agenten hergestellt wurde
Koordinationsrechner	Alle	Agent	443	HTTPS	Jetty	Web-Socket-Verbindung, die von Agenten hergestellt wurde

Von Agenten verwendete Ports

Die folgenden Tabellen bieten eine Übersicht über die Ports, die für die Kommunikation von und zu CA Process Automation-Agenten verwendet werden.

Kommunikation von einem Agenten

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Agent	Alle	Koordinationsrechner	8080	HTTP	tomcat.connector.http.port	CA Process Automation-Benutzeroberfläche - Port für einfache Kommunikation.
Agent	Alle	Koordinationsrechner	8443	HTTPS	tomcat.secure.port	CA Process Automation-Benutzeroberfläche - Port für sichere Kommunikation.
Agent	Alle	Apache-Lastenausgleich	80	HTTP	Apache httpd.conf	Port des Apache-Lastenausgleichs für einfache Kommunikation
Agent	Alle	Apache-Lastenausgleich	443	HTTPS	Apache httpd.conf	Port des Apache-Lastenausgleichs für sichere Kommunikation
Agent	Alle	Koordinationsrechner	7001	HTTP/ HTTPS	oasis.jxta.port	Veralteter Serverport
Agent	Alle	Koordinationsrechner	80	HTTP	Jetty	Serverport
Agent	Alle	Koordinationsrechner	443	HTTPS	Jetty	Serverport
Agent	Alle	Ziel-Remote-Host	22	TCP	Standardmäßiger SSH-Port	Für SSH-Kommunikation mit einem Proxy-Kontaktpunkt oder einer Hostgruppe verwendet.

Kommunikation zu einem Agenten

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Agent	7003	HTTP/ HTTPS	Skript für Agenteninstallation	Agent hat zuvor diesen veralteten Port für die Kommunikation mit Koordinationsrechnern überwacht.
Koordinationsrechner	Alle	Agent	80	HTTP	Jetty	Web-Socket-Verbindung, die von Agenten hergestellt wurde
Koordinationsrechner	Alle	Agent	443	HTTPS	Jetty	Web-Socket-Verbindung, die von Agenten hergestellt wurde

Von Datenbankservern verwendete Ports

Die folgende Tabelle bietet eine Übersicht über die Ports, die für die Kommunikation zu einem Datenbankserver verwendet werden.

Kommunikation zu einem Datenbankserver

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Microsoft SQL-Datenbankserver	1433	TCP	In Microsoft SQL konfiguriert	Der Datenbankport kann in der Installation des Datenbankservers geändert werden. Der Standardwert ist 1433.
Koordinationsrechner	Alle	MySQL-Datenbankserver	3306	TCP	In MySQL konfiguriert	Der Datenbankport kann in der Installation des Datenbankservers geändert werden. Der Standardwert ist 3306.

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Koordinationsrechner	Alle	Oracle-Datenbankserver	1521	TCP	In Oracle konfigurierter Listener	Der Datenbankport kann im Schritt "Create Listener" geändert werden. Der Standardwert für den Oracle Listener-Port ist 1521. Die Datenbankinstanz kann zu einem anderen Listener zugeordnet werden. Konsultieren Sie die Oracle-Konfiguration.

Von Web-Clients verwendete Ports

Die folgende Tabelle bietet eine Übersicht über die Ports, die für die Kommunikation von Web-Clients verwendet werden.

Kommunikation von Web-Clients

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Webbrowser (CA EEM-Administrator)	Alle	CA EEM	5250	TCP	CA EEM-Konfiguration	Webbrowser, der auf die CA EEM-Benutzeroberfläche zugreift.
Webbrowser (CA Process Automation-Anwender)	Alle	Apache-Lastenausgleich	80	TCP	Apache httpd.conf	Port des Apache-Lastenausgleichs für einfache Kommunikation
Webbrowser (CA Process Automation-Anwender)	Alle	Apache-Lastenausgleich	443	TCP	Apache httpd.conf	Port des Apache-Lastenausgleichs für sichere Kommunikation

Von:	Port	An	Standardmäßiger Abhör-Port	Protokoll	Konfiguration	Beschreibung
Webservices-Client (SOAP)	Alle	Apache-Lastenausgleich	80	TCP	Apache httpd.conf	Port des Apache-Lastenausgleichs für einfache Kommunikation
Webservices-Client (SOAP)	Alle	Apache-Lastenausgleich	443	TCP	Apache httpd.conf	Port des Apache-Lastenausgleichs für sichere Kommunikation
Catalyst-REST-Client	Alle	Apache-Lastenausgleich	7000	HTTP	node0-config.xml, http.port	Port des CA Process Automation-Catalyst-Containers
Catalyst-REST-Client	Alle	Apache-Lastenausgleich	7443	HTTPS	node0-config.xml, https.port	Sicherer Port des CA Process Automation-Catalyst-Containers
Webbrowser (CA Catalyst-Administrator)	Alle	Koordinationsrechner	8181	TCP	ucf.pax.web.http.port	Catalyst-Karaf-Admin-Benutzeroberfläche - In normalen Vorgängen nicht verwendet.

Anhang C: Verwalten des DNS-Namen oder der IP-Adresse des Koordinationsrechners

Dieses Kapitel enthält folgende Themen:

Verwalten von IP-Adressen (siehe Seite 253)
Korrigieren von ungültigen Zeichen im CA Process Automation-DNS-Namen (siehe Seite 254)

Verwalten von IP-Adressen

Möglicherweise ist das Verwalten von IP-Adressen erforderlich. Einige Beispiele:

- Ändern der IP-Adresse und Namen eines Koordinationsrechners.

  Ändern Sie die Kombination der Namen und IP-Adresse, unabhängig davon, wo sie in folgenden Dateien angezeigt werden.

  Installationsverzeichnis`/server/c2o/.config/OasisConfig.properties`

  Installationsverzeichnis`/server/c2o/.config/Domain.xml`

  Hinweis: Um weiterhin einen unveränderten Hostnamen in allen Referenzen in CA Process Automation zu verwenden, ändern Sie das DNS mit der neuen IP-Adresse.

- Wenn Sie Agenten mithilfe von geänderten IP-Adressen installieren, konfigurieren Sie den Agenten neu, indem Sie folgende Datei aktualisieren:

  Installationsverzeichnis`/PAM Agent/PAMAgent/.config/OasisConfig.properties`

  Ändern Sie den Wert der folgenden Eigenschaft:

  `oasis.jxta.host`

- Verwenden Sie mehrere IP-Adressen für CA Process Automation, wenn Sie zwei NICs haben, eine interne und eine andere externe.

  Damit CA Process Automation an die externe IP-Adresse gebunden wird, fügen Sie der Datei "OasisConfig.properties" folgende Eigenschaft hinzu:

  `jboss.bind.address=`*`xxx.xxx.xxx.xxx`*

Korrigieren von ungültigen Zeichen im CA Process Automation-DNS-Namen

In Version 3.1 akzeptierte CA Process Automation die Installation von Koordinationsrechnern mit DNS-Namen, die eingeschränkte Zeichen, wie z. B. Unterstriche (_), enthielten.

Wenn Sie einen Koordinationsrechner mit einem ungültigen Hostnamen installiert haben, müssen Sie folgende Korrekturmaßnahmen vornehmen:

1. Erstellen Sie einen DNS-Datensatz, der den korrigierten Hostnamen zu seiner IP-Adresse zuordnet.

   Weitere Informationen zu Standards finden Sie unter Syntax für DNS-Hostnamen (siehe Seite 256).

2. Erstellen Sie einen DNS-Datensatz, der den falschen Namen dem korrigierten Namen zuordnet.

   Weitere Informationen finden Sie unter Aktivieren von DNS zur Behebung von ungültigen Hostnamen (siehe Seite 254).

3. Aktualisieren Sie die Datei "OasisConfig.properties" mit dem korrigierten Namen.

   Weitere Informationen finden Sie unter Verwalten der DNS-Hostnamen (siehe Seite 255).

Aktivieren von DNS zur Behebung von ungültigen Hostnamen

Wenn Sie einen Koordinationsrechner mit einem Hostnamen erstellt haben, der einen Unterstrich oder ein anderes ungültiges Zeichen enthält, können Sie Schritte vornehmen, durch die der DNS-Server die korrekte IP-Adresse von einem ungültigen Hostnamen ermittelt. Dafür ist es erforderlich, dass Sie zwei Datensätze im DNS-Server erstellen. Der erste Datensatz gibt an, dass der ursprüngliche ungültige Name ein Alias eines anderen kanonischen Namens ist.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie im Domain Name System einen kanonischen Datensatz mit einem neuen und gültigen Hostnamen.
2. Erstellen Sie einen CNAME-Datensatz, der den kanonischen Namen zum ursprünglichen und ungültigen Namen zuordnet.

Name	Typ	Wert
my_host.mycompany.com.	CNAME	myhost.mycompany.com.
myhost.mycompany.com	A	172.24.36.107

In diesem Beispiel ist "my_host.mycompany.com" ein Alias für den kanonischen Namen (CNAME) "myhost.mycompany.com".

Wenn die DNS-Auflösung einen CNAME-Datensatz findet, während der ursprünglichen Ressourcendatensatz abgefragt wird, dann wird die Abfrage neu gestartet, und anstelle des CNAME wird der ursprüngliche Name verwendet. Der kanonische Name, auf den ein CNAME-Datensatz verweist, kann sich irgendwo im DNS befinden.

Verwalten der DNS-Hostnamen

Sie können den Hostnamen für einen Koordinationsrechner ändern. Wenn der Hostname zum Beispiel nicht der unterstützten Syntax entspricht, können Sie ihn aktualisieren. Wenn Sie CA Process Automation mit einem ungültigen DNS-Hostnamen installiert haben, der eingeschränkte Zeichen enthält, wie z. B. Unterstriche, dann erstellen Sie ein Alias, das den DNS-Standards entspricht. Ersetzen Sie dann den ungültigen Hostnamen manuell durch dieses Alias in Ihrer "OasisConfig.properties"-Datei.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie ein Alias. Weitere Informationen finden Sie unter Aktivieren von DNS zur Behebung von ungültigen Hostnamen (siehe Seite 254).
2. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
3. Navigieren Sie zum folgenden Ordner, wobei "Installationsverzeichnis" für den Installationspfad des Domänen-Koordinationsrechners steht:

   `Installationsverzeichnis/server/c2o/.config`
4. Öffnen Sie die Datei "OasisConfig.properties" mit einem Editor.
5. Verwenden Sie "Suchen", um folgende Eigenschaft zu finden:

   `oasis.local.hostname`
6. Ändern Sie den Wert für die Eigenschaft "oasis.local.hostname=".
7. Speichern Sie die Datei, und schließen Sie den Editor.
8. Starten Sie den Koordinationsrechner-Service neu.
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 142).
   b. Starten Sie den Koordinationsrechner (siehe Seite 143).

Syntax für DNS-Hostnamen

Es gibt viele Standorte, in denen Sie einen FQDN oder eine IP-Adresse eingeben können. Wenn Ihre DNS-Hostnamen einen Unterstrich enthalten oder in irgendeiner Weise nicht der erforderlichen Syntax entsprechen, geben Sie die IP-Adresse an.

Gültige DNS-Hostnamen:

- Beginnen mit einem alphabetischen Zeichen.
- Enden mit einem alphanumerischen Zeichen.
- Enthalten 2-24 alphanumerische Zeichen.
- Können das Sonderzeichen Minus (-) enthalten.

  Wichtig! Das Minuszeichen (-) ist das einzige Sonderzeichen, dass in DNS-Hostnamen erlaubt ist.

Anhang D: Fehlerbehebung

Dieser Abschnitt beschreibt die Fehlerbehebungsmethoden, um CA Process Automation zu verwenden.

Dieses Kapitel enthält folgende Themen:

Fehlschlagen der CA Process Automation-Installation (siehe Seite 257)
Potenzielles Problem wenn CA Process Automation auf einem VMWare-Server mit einer E1000-Netzwerkschnittstelle ausgeführt wird (siehe Seite 258)
Oracle-Fehlernummer 9347941 (siehe Seite 260)
Beschränkungen in Internet Explorer (siehe Seite 261)
CA Process Automation-Installation in Netzwerkumgebungen mit dualem Stapel (IPv4 und IPv6) (siehe Seite 262)
Unbefriedigende Leistung bei Verwendung von MySQL (siehe Seite 262)
Erstellen der Laufzeitdatenbank nicht möglich (siehe Seite 264)
Die Operatoren "Skript ausführen" und "Programm ausführen" können nicht auf RHEL6 ausgeführt werden (siehe Seite 265)

Fehlschlagen der CA Process Automation-Installation

Symptom:

Wenn der erste Versuch der CA Process Automation-Installation fehlschlägt, werden darauffolgende Versuche, CA Process Automation am gleichen Speicherort zu installieren, auch fehlschlagen.

Lösung:

Um CA Process Automation erneut zu installieren, bereinigen Sie die verbliebenen Registrierungseinträge, Dateien und Ordner an jenem Speicherort, bevor Sie mit der Installation beginnen, oder verwenden Sie einen anderen Speicherort.

Potenzielles Problem wenn CA Process Automation auf einem VMWare-Server mit einer E1000-Netzwerkschnittstelle ausgeführt wird

Symptom:

Die Ursachen dieses Problems sind in seltenen Fällen Socket-I/O-Fehler, die dazu führen können, dass die Software unbeschränkt auf den Abschluss des Lesevorgangs wartet.

Für die Anwender sind die normalen Symptome das unerwartete Hängen von Prozessen, die normalerweise ohne Issue abgeschlossen werden. Diese Prozesse werden nach einem Neustart des CA Process Automation-Koordinationsrechners erwartungsgemäß abgeschlossen. Dies kann einen kleinen Teil der Prozesse oder alle ausgeführten Prozesse betreffen. Es besteht kein Zusammenhang mit der Betriebszeit des Koordinationsrechners und kann kurz nach einem Neustart oder nach Tagen, Wochen oder Monaten einwandfreier Koordinationsrechnerfunktion auftreten.

Dieses Problem wurde nur in Umgebungen beobachtet, die hohe Volumes an CA Process Automation-Prozessen ausführen. In den meisten Umgebungen, in denen "E1000 NIC" installiert ist, ist das Problem nie aufgetreten, oder es ist so selten aufgetreten, dass es nicht entdeckt wurde.

Lösung:

Dieses Problem ist sehr schwierig zu bestätigen. Wenn dieses Problem auftritt, wird der CA Process Automation-Thread oft auf einem Socket-Lesevorgang blockiert, und es werden keine relevanten Fehler in die Protokolldateien geschrieben. Die Bestätigung des Problems erfordert das Überprüfen von mehreren Java-Thread-Speicherauszügen, die beim Auftreten dieses Problems aufgezeichnet werden, um zu bestätigen, dass der Operator bei einem Socket-Lesevorgang blockiert wird.

Wenn Fehler im Zusammenhang mit diesem Problem beobachtet werden, werden häufig generische Verbindungsfehler angezeigt, die andere berechtigte und nicht verwandte Ursachen haben könnten. Folgendes Beispiel:

```
2013-07-24 18:55:23.219 WARN  [org.hibernate.jdbc.AbstractBatcher]
[nPool Worker-23] exception clearing maxRows/queryTimeout
com.microsoft.sqlserver.jdbc.SQLServerException: The connection is
closed.
                at
com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverErro
r(Unknown Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerConnection.checkClosed(Unkno
wn Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.checkClosed(Unknow
n Source)
```

```
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.getMaxRows(Unknown
Source)
                at
org.jboss.resource.adapter.jdbc.CachedPreparedStatement.getMaxRows
(CachedPreparedStatement.java:367)
                at
org.jboss.resource.adapter.jdbc.WrappedStatement.getMaxRows(Wrappe
dStatement.java:378)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:272)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:209)
```

. . . und so weiter.

In diesen Fällen ist Identifizierung des Problems vorläufig, und andere Gründe für Kommunikationsfehler müssen ausgeschlossen werden.

Häufige Prozessfehler oder ein wiederholbarer Fehler eines individuellen Operators oder von Operatoren zeigen wahrscheinlich andere nicht verwandte Probleme innerhalb des Prozessdesigns oder der Koordinationsrechnerfunktion an.

Bei Sites, wo dieses Problem bestätigt wurde, wird die Neukonfiguration des VMWare-Servers von einem "E1000 Network Interface Card"-Treiber auf einen "VMXnet-3 NIC"-Treiber als wirksame Minimierung des Problems angesehen.

CA Technologies zögert, dies als vollständige Lösung zu deklarieren, da die Incident-Rate sehr gering ist und der Zeitraum zwischen den Vorkommen (auch mit "E1000 NIC") sehr lang sein kann.

Wenn eine Überprüfung des Issues vor dem Durchführen dieser Änderung erforderlich ist, kontaktieren Sie den Support, um die Protokollierung und Java-Thread-Speicherauszüge einzurichten, die erforderlich sind, um die Fehlerbehebung für diesen bestimmten Issue durchzuführen.

Oracle-Fehlernummer 9347941

Wichtig! Wenn Versionen von Oracle-RDBMS ausgeführt werden, die vor der Version 11.1.0.7 liegen, dann tritt bei CA Process Automation der bekannte Oracle-RDBMS-Defekt 9347941 auf, bei dem das gleichzeitige Einfügen von CLOB-Daten, bei denen die individuellen Spaltenwerte die Größe von 52 KB überschreiten, gelegentlich dazu führt, dass diese Spalten mit Daten über dem 52K-Offset, das durch Leerzeichen ersetzt wird, falsch aktualisiert werden. Dieses Problem wurde sowohl bei der Verwendung von 10g-Versionen als auch bei früheren 11g-Versionen von Oracle-RDBMS beobachtet.

Symptom:

Der CA Process Automation-Prozess würde abstürzen. Sie müssen den Prozess am entsprechenden Operator zurücksetzen, wo der Prozess abgestürzt ist, um mit der abzuschließenden Prozessausführung fortzufahren. Das Problem ist selten und wurde nur bei äußerst hohen Aktualisierungskonflikten beobachtet.

Lösung:

Dieses Problem wurde nicht beobachtet, wenn entweder Version 11.1.0.7 oder 11.2.0.2 von Oracle ausgeführt wird. Es wird empfohlen, dass Standorte, die Oracle für ihre CA Process Automation-Datenbanken verwenden, Version 11.1.0.7 oder 11.2.0.2 oder höher ausführen.

Beschränkungen in Internet Explorer

Internet Explorer beschränkt die Agenteninstallation in einem Netzwerk, das nicht dem Netzwerk entspricht, auf dem der Domänen-Koordinationsrechner installiert ist.

Symptom:

Greifen Sie auf den Domänen-Koordinationsrechner mithilfe von Internet Explorer zu, und installieren Sie den CA Process Automation-Agenten in einem Netzwerk, das nicht dem Netzwerk entspricht, auf dem der Domänen-Koordinationsrechner installiert ist. Die Installation kann fehlschlagen, während JAR-Dateien für die Installation heruntergeladen werden.

Lösung:

Die mögliche Ursache dieses unregelmäßig auftretenden Problems könnte sein, dass Java JAR-Dateien während der Weiterleitung durch den Proxy in Internet Explorer nicht laden kann. Ändern Sie zum Minimieren des Problems die Java-Netzwerkeinstellungen in "Direktverbindung", bevor Sie den Agenten installieren.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie die Java-Systemsteuerung auf dem Hostsystem, auf dem Sie den Agenten installieren.
2. Öffnen Sie auf der Registerkarte "Allgemein" die Option "Netzwerkeinstellungen".

   Die Seite "Netzwerkeinstellungen" wird angezeigt.
3. Wählen Sie die Option "Direktverbindung" aus, und klicken Sie auf "OK", um die Änderungen zu speichern.
4. Installieren Sie den Agenten.

CA Process Automation-Installation in Netzwerkumgebungen mit dualem Stapel (IPv4 und IPv6)

Wenn Sie CA Process Automation in Netzwerkumgebungen mit dualem Stapel (IPv4 und IPv6) installieren, kann CA Process Automation möglicherweise nicht gestartet werden.

Symptom:

Wenn Sie CA Process Automation in Netzwerkumgebungen mit dualem Stapel (IPv4 und IPv6) installieren, treten möglicherweise Probleme auf, während auf die folgenden CA Process Automation-Komponenten über das Netzwerk zugegriffen wird:

- Domänen-Koordinationsrechner
- Koordinationsrechner
- Agenten

Lösung:

Deaktivieren Sie den IPv6-Stapel auf dem Hostsystem, auf dem eine oder mehrere der folgenden CA Process Automation-Komponenten ausgeführt werden, und starten Sie die Dienste neu:

- Domänen-Koordinationsrechner
- Koordinationsrechner
- Agenten

Unbefriedigende Leistung bei Verwendung von MySQL

Symptom:

Wenn ich CA Process Automation mit MySQL oder Oracle als Datenbank installiere, bemerke ich eine Verschlechterung des Leistungsverhaltens.

Lösung:

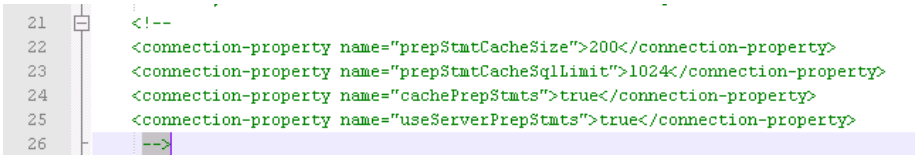
Ändern Sie nach der Installation die Datei oasis-ds.xml, um die Leistung von CA Process Automation verbessern.

Gehen Sie folgendermaßen vor:

1. Suchen und öffnen Sie die Datei oasis-ds.xml in:

   Installationsverzeichnis/Server/c2o/ext-deploy

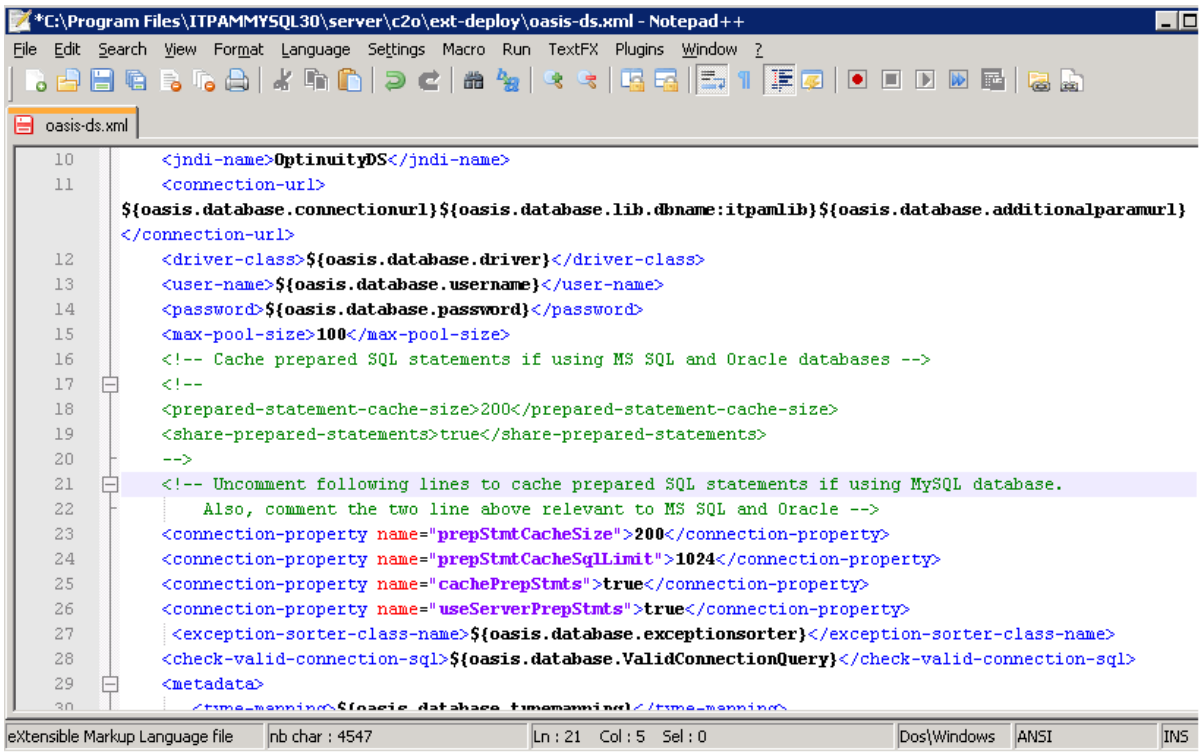
2. Entfernen Sie die Kommentarzeichen am Anfang der folgenden Zeilen:



3. Fügen Sie am Anfang der folgenden Zeilen Kommentarzeichen ein:

```
16      <!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
17      <prepared-statement-cache-size>200</prepared-statement-cache-size>
18      <share-prepared-statements>true</share-prepared-statements>
```

Die aktualisierte Datei sollte wie folgt aussehen:



4. Starten Sie den Koordinationsrechner neu.

Erstellen der Laufzeitdatenbank nicht möglich

Symptom:

Wenn ich einen Koordinationsrechner installiere und die Laufzeitdatenbank im Fenster "Laufzeitdatenbank" angebe, wird die folgende Ausnahme ausgegeben:

```
Die Laufzeitdatenbank wird von einem anderen Koordinationsrechner verwendet.
```

Lösung:

In Version 4.0 von CA Process Automation können Sie eine Laufzeitdatenbank nicht für mehrere Koordinationsrechner gemeinsam verwenden. Normalerweise können Sie dieses Problem lösen, indem Sie die Laufzeitdatenbank mit einem anderen Namen erstellen oder wenn die Laufzeitdatenbank von einem separaten Datenbankserver gehostet wird.

Verwenden Sie folgenden Vorgang **nur dann**, wenn Sie die Laufzeitinformationen in dieser Datenbank in einer neuen CA Process Automation-Instanz beibehalten möchten. Dies ist selten der Fall, und das Zurücksetzen von "RuntimeDbOrchestratorID" hat viele unerwünschte Nebeneffekte. Einer dieser Nebeneffekte ist, dass ausgeführte Operatoren in dieser Laufzeitdatenbank nicht abgeschlossen werden können. Unter anderem müssen alle Agenten und sekundären Koordinationsrechner auch neu installiert werden. Wenn Sie nicht sicher sind, ob dies der geeignete Vorgang für Ihr Problem ist, wenden Sie sich an den technischen Support, bevor Sie fortfahren.

In dieser Version wird in der Datenbank eine neue Eigenschaftstabelle mit den folgenden Spalten erstellt:

- PropKey
- PropValue

Wenn ein Koordinationsrechner eine Laufzeitdatenbank verwendet, wird eine neue Zeile in der Eigenschaftstabelle eingefügt. PropKey ist RuntimeDbOrchestratorID und PropValue ist die eindeutige ID des Koordinationsrechners.

Wenn ein anderer Koordinationsrechner die gleiche Datenbank anfordert, wird die Datenbank in der Eigenschaftstabelle validiert. Wenn die eindeutige ID des anfordernden Koordinationsrechners nicht dem PropValue ähnelt, wird die folgende Meldung angezeigt:

```
Die Laufzeitdatenbank wird von einem anderen Koordinationsrechner verwendet.
```

Wichtig! Die Einträge der Laufzeitdatenbank werden selbst nach der Deinstallation des Produkts nicht gelöscht.

Um die gleiche Datenbank erneut für Laufzeit zu verwenden, führen Sie die folgende SQL-Abfrage aus, und löschen Sie die entsprechende Zeile aus der Eigenschaftstabelle.

```
Löschen Sie aus Eigenschaften, wenn propkey = 'RuntimeDbOrchestratorID'
```

Die Operatoren "Skript ausführen" und "Programm ausführen" können nicht auf RHEL6 ausgeführt werden

Symptom:

Die Operatoren "Skript ausführen" und "Programm ausführen" schlagen fehl, wenn sie auf RHEL6 ausgeführt werden.

Lösung:

Die Operatoren "Skript ausführen" und "Programm ausführen" suchen die Korn-Shell (ksh), wenn sie auf UNIX- oder Linux-Plattformen ausgeführt werden. Standardmäßig ist ksh nicht auf RHEL 6 installiert.

Dieses Problem kann behoben werden, indem Sie eine dieser Optionen befolgen:

- Installieren Sie ksh:

  Sie können ksh mit folgendem Befehl installieren:

  ```
  yum install ksh
  ```

- Verweisen Sie eine symbolische Verknüpfung zu einer gültigen Shell

  Erstellen Sie die symbolische Verknüpfung "/bin/ksh", und ordnen Sie einer Shell (wie z. B. Bash) die gleiche Verknüpfung zu, die auf diesem Computer vorhanden ist. Verwenden Sie diesen Befehl, wobei "/bin/bash" der Speicherort der Bash-Shell ist:

  ```
  ln -s /bin/bash /bin/ksh
  ```

Anhang E: Apache-Lastenausgleich

Der Apache-Lastenausgleich *unterstützt nicht* die vereinfachte Kommunikation für Agenten. Um die Vorteile der vereinfachten Kommunikation nutzen zu können, müssen Sie NGINX oder einen anderen Web-Socket-basierten Lastenausgleich verwenden. Wenn Sie die veraltete Kommunikationsmethode verwenden, verwenden Sie diese Anweisungen, um den Apache-Lastenausgleich zu installieren und zu konfigurieren.

Weitere Informationen finden Sie unter "Informationen zur Agent-Kommunikation (siehe Seite 164)".

Voraussetzungen des Apache-Lastenausgleichs

Ein *geclusterter Koordinationsrechner* ist ein Satz an Knoten, die angezeigt werden und als ein allein stehender Koordinationsrechner agieren und eine gemeinschaftlich genutzte Bibliothek verwenden. Sie können einen CA Process Automation-Koordinationsrechner für Hochverfügbarkeit, Fehlertoleranz und Skalierbarkeit clustern.

Ein Lastenausgleich, wie z. B. der Apache-HTTP-Server, ist für das Clustering eines Koordinationsrechners, einschließlich des Domänen-Koordinationsrechners, erforderlich. Ein Lastenausgleich ist kein Teil der CA Process Automation-Installation.

Während der Lastenausgleich auf dem gleichen Host wie einer der Koordinationsrechner-Knoten konfiguriert werden kann, befindet sich der Lastenausgleich üblicherweise auf einem separaten Host.

Ein Lastenausgleich wird *nur* für einen Koordinationsrechner in einer geclusterten Konfiguration und in bestimmten Single-Sign-On-Konfigurationen (SSO) erforderlich.

Wichtig! Wenn ein Koordinationsrechner installiert wird, ohne dabei zunächst einen Lastenausgleich zu installieren und zu konfigurieren, kann dieser Koordinationsrechner nicht später clustern.

Apache-Lastenausgleichs-Konfiguration unter Windows

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs unter Windows enthalten.

Sie können die folgenden zwei Modi konfigurieren:

- Grundlegende Konfiguration (Windows) (siehe Seite 268)
- Sichere Konfiguration (Windows) (siehe Seite 272)

Grundlegende Konfiguration (Windows)

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs im grundlegenden Modus enthalten.

Hinweis: Statt Apache können Sie einen anderen Lastenausgleich verwenden. Allerdings ist es für einen CA Process Automation-Koordinationsrechner erforderlich, dass einige Anfrageklassen an einen bestimmten Knoten im geclusterten Koordinationsrechner geleitet werden. Deswegen ist ein einfacher Lastenausgleich nicht ausreichend. Informationen zu Alternativen finden Sie auf der Seite mit den Best Practices für die CA Process Automation-Implementierung, oder kontaktieren Sie den CA Support, um Hilfe zu erhalten. Das Bookshelf enthält Verknüpfungen zu diesen Seiten.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (Windows) (siehe Seite 268).
2. Konfigurieren der einfachen Kommunikation (siehe Seite 270).
3. (Optional) Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Windows) (siehe Seite 271)

   Hinweis: Damit der Apache-Webserver HTTPS-Anforderungen an Catalyst-Operatoren weiterleiten kann, müssen die SSL-Zertifikate das PEM-Format aufweisen. Bei Bedarf: Generieren von SSL-Zertifikatsdateien (siehe Seite 51).

Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (Windows)

Der CA Process Automation-Installationsdatenträger enthält Beispielkonfigurationsdateien für den Apache-Lastenausgleich, den Sie als Ausgangspunkt für die Konfiguration verwenden können:

```
ApacheConfig.zip
```

Folgende Anweisungen gehen davon aus, dass ein Lastenausgleich von Apache 2.2 an CA Process Automation zugewiesen ist. Installieren Sie zunächst einen Apache-Lastenausgleich. Extrahieren Sie anschließend die Dateien aus der CA Process Automation-ZIP-Datei "ApacheConfTemplates" in den Ordner "Conf" unter dem Installationsverzeichnis von Apache.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich am Host an, auf dem der Lastenausgleich ausgeführt werden soll.

   Der Lastenausgleich befindet sich normalerweise nicht auf dem gleichen Host wie Ihr Domänen-Koordinationsrechner. Allerdings muss der Host mit Ihrem Domänen-Koordinationsrechner vom Lastenausgleich routingfähig sein.
2. Laden Sie den aktuellsten Apache-Lastenausgleich herunter, und installieren Sie mit SSL-Unterstützung. Befolgen Sie die Anweisungen des Anbieters.

3. Laden Sie folgende Datei für die Apache-Version herunter, die Sie installiert haben:

   `mod_jk.so`

   Wir empfehlen, dass Sie die aktuellste Version herunterladen.

4. Kopieren Sie die Date "mod_jk.so" in den folgenden Ordner:

   `apache_Installationsverzeichnis``\modules`

5. Navigieren Sie zum folgenden Ordner auf dem CA Process Automation-Installationsdatenträger:

   `Installationsverzeichnis``\DVD1\ApacheConfTemplates`

6. Extrahieren Sie die folgenden Dateien aus "ApacheConfig.zip":

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   `httpd VIRTUALHOST_EXAMPLE FILE`

   Hinweis: Die extrahierte Datei "httpd VIRTUALHOST_EXAMPLE" enthält Text, den Sie ausschneiden und in die httpd-Datei von Apache einfügen können, wenn Sie sichere Kommunikationen konfigurieren. Der erforderliche Text ist auch in der Dokumentation.

7. Kopieren Sie die folgenden extrahierten Dateien in den Ordner "*apache_install_dir*\conf":

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   Hinweis: Wenn Sie keinen zuzuweisenden Lastenausgleich von Apache 2.2 haben, führen Sie die Konfigurationsinformationen in den Eigenschaften der Beispielvorlage und die Conf-Dateien in Ihre vorhandenen Dateien zusammen. Führen Sie vorsichtshalber eine Sicherung Ihrer Dateien durch, bevor Sie sie ändern.

Konfigurieren der einfachen Kommunikation

Sie können einen Lastenausgleich für einfache Kommunikation mit den Knoten des Domänen-Koordinationsrechners oder anderen Koordinationsrechner konfigurieren.

Gehen Sie folgendermaßen vor:

1. Wechseln Sie zum folgenden Ordner:

   Apache_Installationsverzeichnis\conf

   Dieser Ordner enthält "worker.properties" und "mod-jk.conf".

2. Öffnen Sie die Datei "workers.properties".
3. Fügen Sie den ersten Knoten hinzu, indem Sie "node1" definieren, das mit der folgenden Zeile beginnt:
   `worker.`**`node1`**`.host=<Enter node1 hostname here>`
4. Ersetzen Sie den Platzhalter *Enter node1 hostname here* von dieser Zeile für "worker.node1.host" mit dem gültigen Wert.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.
5. Speichern und schließen Sie die Datei "worker.properties".
6. Öffnen Sie die Datei "mod-jk.conf".
7. Heben Sie die Auskommentierung der folgenden Zeile auf:

   `# JkMountFile conf/uriworkermap.properties`
8. Speichern und schließen Sie die Datei "mod-jk.conf".
9. Öffnen Sie die Datei "httpd.conf".
10. Fügen Sie die folgenden Eintrag am Ende der Datei "httpd.conf" ein:
    ```
    #Lastenausgleichsmodul
    Include conf/mod-jk.conf
    ```
11. Speichern und schließen Sie die Datei "httpd.conf".

Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Windows)

Sie können den Apache-Webserver (Lastenausgleich) für Catalyst RESTful API konfigurieren. Die Apache-Konfigurationsänderungen basieren auf dem Apache-Lastenausgleich, der für CA Process Automation bereits konfiguriert ist.

Nachdem Sie CA Process Automation in einem Clustermodus konfiguriert haben, führen Sie die Aufgaben nach der Installation aus.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zum folgenden Ordner auf dem Installationsdatenträger von CA Process Automation:

   Installationsverzeichnis\DVD1\ApacheConfTemplates

2. Extrahieren Sie die folgenden Dateien aus "ApacheConfig.zip":

   `httpd-proxy.conf`

3. Kopieren Sie die Datei "httpd-proxy.conf" zu "*apacheHome*/conf/extra directory".

4. Aktualisieren Sie die folgenden Zeilen sowohl in "HTTP Virtual Hosts" als auch in "HTTPS Virtual Hosts", um die Koordinationsrechner-Hostnamen für "BalancerMember" zu ersetzen.

   Ungesicherte Node-Members

   ```
   <Proxy balancer://ucfcluster>
   BalancerMember  http://< Enter node1 hostname>:7000
   BalancerMember  http://< Enter node2 hostname>:7000
   ```

   Gesicherte Node-Members

   ```
   <Proxy balancer://sslcluster>
   BalancerMember  https://< Enter node1 hostname>:7443
   BalancerMember  https://< Enter node2 hostname>:7443
   ```

5. Ersetzen Sie den Platzhalter "<Enter node*x* hostname here>" für "worker.node*x*.host" durch den gültigen Wert.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

6. Speichern Sie die Datei httpd-proxy.conf.

7. Öffnen Sie die Datei "*apacheHome*/conf/httpd.conf", und stellen Sie sicher, dass die Ports 7000 und 7443 nicht verwendet werden.

8. Fügen Sie die folgende Zeile am Ende der Datei "httpd.conf" ein:

   `Include conf/extra/httpd-proxy.conf`

9. Folgen Sie dem Verfahren unter Generieren von SSL-Zertifikatsdateien (siehe Seite 51), um "c2okey2.pem"- und "c2ocert.pem"-Dateien zu generieren.
10. Kopieren Sie die generierten Dateien in das Verzeichnis "*apacheHome/*conf".
11. Speichern Sie die geänderten Dateien, und starten Sie den Apache-Webserver neu.

Sichere Konfiguration (Windows)

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs im sicheren Modus enthalten.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (siehe Seite 268).
2. Generieren von SSL-Zertifikatsdateien (siehe Seite 51)

   Hinweis: Damit der Apache-Webserver HTTPS-Anfragen an Catalyst-Operatoren weiterleiten kann, müssen die SSL-Zertifikate dem PEM-Format entsprechen.
3. Konfigurieren der sicheren Kommunikation (Windows) (siehe Seite 275).
4. Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Windows) (siehe Seite 271)

Generieren von SSL-Zertifikatsdateien

Die SSL-Zertifikate müssen *nach* der Installation von CA Process Automation und *vor* der Konfiguration von sicherer Kommunikation für Ihren Lastenausgleich generiert werden. SSL-Zertifikate sind nicht erforderlich, wenn Sie für Ihren Lastenausgleich grundlegende, nicht sichere Kommunikation verwenden möchten.

Nachdem das Zertifikat generiert wurde, muss der Speicherort der Zertifikatsdatei identifiziert werden, wenn Sie Ihren Lastenausgleich für sichere Kommunikation konfigurieren.

Gehen Sie folgendermaßen vor:

1. Laden Sie OpenSSL von einem Drittanbieter herunter, und installieren Sie es.

   Hinweis: Stellen Sie sicher, dass auf dem Host, auf dem Sie OpenSSL installieren, JDK installiert ist.

2. Nachdem Sie CA Process Automation im Clustermodus installiert haben (und mindestens ein Knoten installiert wurde), generiert der CA Process Automation-Installationsassistent die Datei "c2okeystore" am folgenden Speicherort:

   `\server_location\c2o\.config`

   Kopieren Sie die Datei "c2okeystore", und fügen Sie sie im folgenden Verzeichnis ein:

   `\jdk_location\bin`

   Sie können die Befehle lokal von diesem Speicherort aus ausführen.

3. Verwenden Sie "keytool" in JDK, um den Schlüsselspeicher wie folgt in das pksc12-Format zu importieren:

   a. Gehen Sie zum Verzeichnis "jdk_location\bin", und führen Sie den folgenden Befehl aus:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      Sie werden in der Konsole aufgefordert, das Kennwort des Zielschlüsselspeichers einzugeben.

      Hinweis: Das Schlüsselspeicherkennwort befindet sich in der Datei "OasisConfig.properties". Suchen Sie die Datei im folgenden Verzeichnis: `\server_location\c2o\.config\`

      Öffnen Sie die Datei, und kopieren Sie das Kennwort. Der Wert befindet sich neben der Eingabe "KEYSTOREID=".

      Beispiel: KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. Das Kennwort ist 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Fügen Sie das Kennwort in die Aufforderung zur Eingabe des Zielschlüsselspeicher-Kennworts in Ihrer offenen Konsole ein.

   c. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort wiederholt ein.

   d. Geben Sie das Kennwort in der Aufforderung zur Eingabe des Quellschlüsselspeicher-Kennworts erneut ein.

      Im Verzeichnis \jdk_location\bin wird eine Datei namens "c2okeystore.p12" generiert.

   e. Sie müssen den Schlüsselspeicher im p12-Format in Schlüssel- und Zertifikatsdateien im PEM-Format konvertieren. Führen Sie dazu im Verzeichnis \jdk_location\bin den Befehl "openssl" aus:

```
openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
```

f. Geben Sie das Schlüsselspeicherkennwort in der Aufforderung zur Eingabe des Kennworts ein.

g. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase eine beliebige Phrase ein.

h. Geben Sie Ihre PEM-Passphrase erneut ein.

i. Führen Sie den folgenden Befehl im Verzeichnis \jdk_location\bin aus:
```
openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem
```

j. Geben Sie das Schlüsselspeicherkennwort in der Aufforderung zur Eingabe des Kennworts ein.

k. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase dieselbe Phrase ein, die in Schritt g erstellt haben.

l. Geben Sie Ihre PEM-Passphrase erneut ein.

m. Führen Sie den folgenden Befehl im Verzeichnis \jdk_location\bin aus:
```
openssl rsa -in c2okey.pem -out c2okey2.pem
```

n. Geben Sie in der Aufforderung zur Eingabe der PEM-Passphrase dieselbe Phrase ein, die in Schritt g erstellt haben.

o. Geben Sie Ihre PEM-Passphrase erneut ein.

p. Kopieren Sie die Dateien "c2okey2.pem" und "c2ocert.pem" in das Verzeichnis \conf Ihres Lastenausgleichs.

Hinweis: Erstellen Sie Sicherheitskopien dieser Dateien.

Konfigurieren der sicheren Kommunikation (Windows)

Sie können einen Lastenausgleich für sichere Kommunikation konfigurieren. In den folgenden Schritten gibt *certloc* den Speicherort Ihres Zertifikats an.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (siehe Seite 268).
2. Öffnen Sie die Datei "workers.properties".
3. Fügen Sie den ersten Knoten hinzu, indem Sie "node1" definieren, das mit der folgenden Zeile beginnt:

   ```
   worker.node1.host=<Enter node1 hostname here>
   ```

4. Ersetzen Sie den Platzhalter *Enter node1 hostname here* von dieser Zeile für "worker.node1.host" mit dem gültigen Wert.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

5. Speichern und schließen Sie die Datei "workers".
6. Prüfen Sie CA-Standardspeicherorte in der Datai "openssl" im folgenden Verzeichnis.

   apache_install_location/conf

7. Erstellen oder beziehen Sie eine Zertifikatsdatei und eine private Schlüsseldatei mit einem allgemeinen Namen, der mit dem "ServerName" in "httpd.conf" übereinstimmt.

   Zum Beispiel zeigen die folgenden Schritte, wie Sie das im Apache-Lastenausgleich enthaltene Hilfsprogramm "openssl" verwenden sollten, um eine Zertifikatsdatei zu erstellen. Zusätzliche Optionen steuern den Ablauf des Zertifikats, den Dateinamen und die Algorithmen. Sie können sich auf die vom Anbieter bereitgestellte Dokumentation beziehen, wenn Ihr Standort besondere Anforderungen hat.

   a. Öffnen Sie eine Eingabeaufforderung.

   b. Ändern Sie die Verzeichnisse zum Apache-Ordner "bin".

      cd *apache_install_location*/bin

c. Erstellen Sie eine CSR-Datei (Certificate Signing Request) und PEM-Dateien. Geben Sie dafür folgenden Befehl ein, wobei "mypamserver" ein Name Ihrer Wahl ist:

```
openssl req -config ../conf/openssl.cnf -new -out mypamserver.csr
```

Sie werden aufgefordert, die Passphrase für die PEM-Datei und andere Identifikationsinformationen anzugeben.

- Für die meisten Identifikationsinformationen (Ländernamen, Namen des Bundesstaats/-lands, Namen der Örtlichkeit, Namen der Organisation, Namen der Organisationseinheit) können Sie den Standardwert akzeptieren. Um ein Feld leer zu lassen, geben Sie einen Punkt (.) ein.
- Wenn die Aufforderung für den allgemeinen Namen angezeigt wird, geben Sie als Wert den Teil des Hostnamens von "ServerName" in "*apache_install_location*\conf \httpd.conf" ein.

  Zum Beispiel wenn "ServerName" in httpd.conf den Wert "myhost.mycompany.com:80" hat, geben Sie **myhost.mycompany.com** als allgemeinen Namen an.
- Zu den optionalen Feldern gehören: E-Mail-Adresse, "dir", ein Anfragekennwort und ein optionaler Unternehmensname.

Der Apache-Lastenausgleich erstellt "*mypamserver.*csr" und "*privkey.*pem" im aktuellen Verzeichnis.

d. Erstellen Sie Ihren privaten RSA-Schlüssel. Geben Sie dafür eine Passphrase für "*privkey*.pem" ein, wenn Sie der Apache-Lastenausgleich dazu auffordert.

```
openssl rsa -in privkey.pem -out mypamserver.key
```

e. Erstellen Sie Ihr Zertifikat.

```
openssl x509 -in mypamserver.csr -out mypamserver.cert -req
-signkey mypamserver.key
```

8. Schließen Sie die Eingabeaufforderung, und öffnen Sie Windows Explorer, um generierte Dateien zu kopieren und zu löschen:

   a. Wählen Sie einen "*certloc*"-Ordner aus oder erstellen Sie einen Ordner, um Ihr Zertifikat und die privaten Schlüsseldateien aufzubewahren.

   b. Öffnen Sie den Ordner *apache_install_dir**bin*, wo die Dateien "CERT" und "KEY" generiert wurden.

   c. Ziehen (Verschieben) Sie "*mypamserver*.cert" und "*mypamserver*.key" per Drag-and-drop auf *certloc*.

   d. Löschen Sie die erweiterten Dateien, die im Ordner *apache_install_dir/bin* erstellt wurden. Zu den erweiterten Dateien zählen *mypamserver.CSR*, *privkey.PEM* und ".RND".

9. Sichern Sie die Dateien, die Sie erstellt haben.

10. Ändern Sie mithilfe eines Texteditors die "httpd"-Textdatei ("*apache_install_location*\conf\httpd.conf") folgendermaßen:

    a. Entfernen Sie die Kommentarzeichen am Anfang der folgenden Zeilen:

    ```
    LoadModule rewrite_module modules/mod_rewrite.so

    LoadModule ssl_module modules/mod_ssl.so

    Include conf/extra/httpd-ssl.conf
    ```

    b. Fügen Sie am Ende von "httpd.conf" folgende Zeilen hinzu. Sie können den Text von der Datei "httpd VIRTUALHOST_EXAMPLE" kopieren und einfügen, die Sie aus dem Archiv "SecureDomainConfig_Template.zip" extrahiert haben.

    ```
    <VirtualHost *:80>
    JkMountFile conf/uriworkermap.properties
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
    !^http://.*c2orepository*|MirroringRequestProcessor*|mirror
    ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
    t*
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    </VirtualHost>
    # Load balancing module
    include conf/mod-jk.conf
    ```

    c. Speichern Sie die geänderte "httpd.conf"-Datei, und schließen Sie den Editor.

11. Sichern Sie die Dateien, die Sie bearbeitet haben.

12. Ändern Sie mithilfe eines Texteditors die Konfigurationsdatei *apache_install_location/conf/extra/httpd-ssl.conf* folgendermaßen:
    a. Entfernen Sie das Kommentarzeichen (sofern vorhanden): "Listen 443"
    b. Ändern Sie den "SSLCertificateFile"-Speicherort in ".../*certloc/mypamserver.*cert".

       ```
       SSLCertificateFile "C:/certloc/mypamserver.cert"
       ```

    c. Ändern Sie den "SSLCertificateKeyFile"-Speicherort in ".../*certloc/mypamserver.*key".

       ```
       SSLCertificateKeyFile "C:/certloc/mypamserver.key"
       ```

    d. Fügen Sie die folgenden Zeilen am Ende des <VirtualHost>-Elements hinzu, und zwar vor dem </VirtualHost>-Element:

       ```
       SSLOptions +StdEnvVars +ExportCertData
       JkMountFile conf/uriworkermap.properties
       ```

    e. Speichern Sie die geänderte "httpd.conf-ssl"-Datei, und schließen Sie den Editor.
13. Starten Sie den Apache-Service neu. Klicken Sie dafür im Startmenü auf "Programme", "Apache HTTP Server 2.2", "Control Apache Server" und dann auf "Restart".

    Die Änderungen werden nun wirksam.

Apache-Lastenausgleichs-Konfiguration unter Nicht-Windows-Betriebssystemen

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs unter Nicht-Windows-Betriebssystemen enthalten.

Sie können die folgenden zwei Modi konfigurieren:

- Grundlegende Konfiguration (Nicht-Windows-Betriebssystem) (siehe Seite 279)
- Sichere Konfiguration (Nicht-Windows-Betriebssystem) (siehe Seite 283)

Grundlegende Konfiguration (Nicht-Windows-Betriebssystem)

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs im grundlegenden Modus enthalten.

Hinweis: Statt Apache können Sie einen anderen Lastenausgleich verwenden. Allerdings ist es für einen CA Process Automation-Koordinationsrechner erforderlich, dass einige Anfrageklassen an einen bestimmten Knoten im geclusterten Koordinationsrechner geleitet werden. Deswegen ist ein einfacher Lastenausgleich nicht ausreichend. Informationen zu Alternativen finden Sie auf der Seite mit den Best Practices für die CA Process Automation-Implementierung, oder kontaktieren Sie den CA Support, um Hilfe zu erhalten. Das Bookshelf enthält Verknüpfungen zu diesen Seiten.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (Nicht-Windows-Betriebssystem) (siehe Seite 279).
2. Konfigurieren der einfachen Kommunikation (siehe Seite 270).
3. Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Nicht-Windows-Betriebssystem) (siehe Seite 281)

   Hinweis: Damit der Apache-Webserver HTTPS-Anforderungen an Catalyst-Operatoren weiterleiten kann, müssen die SSL-Zertifikate das PEM-Format aufweisen. Bei Bedarf: Generieren von SSL-Zertifikatsdateien (siehe Seite 51).

Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (Nicht-Windows-Betriebssystem)

Der CA Process Automation-Installationsdatenträger enthält Beispielkonfigurationsdateien für den Apache-Lastenausgleich, den Sie als Ausgangspunkt für die Konfiguration verwenden können:

```
ApacheConfig.zip
```

In den folgenden Anweisungen wird davon ausgegangen, dass ein Lastenausgleich von Apache 2.2 an CA Process Automation zugewiesen ist. Installieren Sie zunächst einen Apache-Lastenausgleich. Extrahieren Sie anschließend die Dateien aus der CA Process Automation-ZIP-Datei "ApacheConfTemplates" in den Ordner "Conf" unter dem Installationsverzeichnis von Apache.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich am Host an, auf dem der Lastenausgleich ausgeführt werden soll.

   Der Lastenausgleich befindet sich normalerweise nicht auf dem gleichen Host wie Ihr Domänen-Koordinationsrechner. Allerdings muss der Host mit Ihrem Domänen-Koordinationsrechner vom Lastenausgleich routingfähig sein.

2. Laden Sie den neuesten Apache-Lastenausgleich herunter, und installieren Sie ihn. Navigieren Sie zum Beispiel zum extrahierten Ordner, und führen Sie die folgenden Befehle aus:

   ```
   ./configure -prefix=<install location>-enable-so -enable-mods-shared=all
   -enable-mod-rewrite --with-z=<zlib home>--with-included-apr  --with-mpm=worker
   --enable-ssl --with-ssl=<ssl home>
   ```

   ```
   Make
   ```

   ```
   Make install
   ```

3. Laden Sie den Tomcat-Connector herunter und installieren Sie ihn, um das "mod_jk"-Modul zu erstellen. Navigieren Sie beispielsweise zu "*<Extrahierter Speicherort des Tomcat Connectors>/native/*", und führen Sie die folgenden Befehle aus:

   ```
   ./configure --with-apxs=<Installationsspeicherort>/bin/apxs
   make
   make install
   ```

4. Stellen Sie sicher, dass der Apache-Webserver aktiv ist und ausgeführt wird.

5. Navigieren Sie zum folgenden Ordner auf dem Installationsdatenträger von CA Process Automation:

   Installationsverzeichnis\DVD1\ApacheConfTemplates

6. Extrahieren Sie die folgenden Dateien aus "ApacheConfig.zip":

   ```
   mod-jk.conf
   ```

   ```
   httpd-proxy.conf
   uriworkermap.properties
   workers.properties
   httpd VIRTUALHOST_EXAMPLE FILE
   ```

   Hinweis: Die extrahierte httpd-Datei enthält Text, den Sie ausschneiden und in die httpd-Datei von Apache einfügen können, wenn Sie sichere Kommunikationen konfigurieren. Der erforderliche Text ist auch in der Dokumentation.

7. Kopieren Sie die extrahierten Dateien in den folgenden Ordner:

   Apache_Installationsverzeichnis\conf

Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Nicht-Windows-Betriebssystem)

Sie können den Apache-Webserver (Lastenausgleich) für Catalyst RESTful API konfigurieren. Nehmen Sie die Apache-Konfigurationsänderungen auf dem Apache-Lastenausgleich vor, der für CA Process Automation bereits konfiguriert ist.

Stellen Sie sicher, dass die folgenden Binärdateien auf dem Apache-Server installiert sind.

```
mod_proxy.so
mod_proxy_balancer.so
mod_proxy_http.so
```

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zum folgenden Ordner auf dem Installationsdatenträger von CA Process Automation:

   Installationsverzeichnis\DVD1\ApacheConfTemplates

2. Extrahieren Sie die folgende Datei aus "ApacheConfig.zip":

   `httpd-proxy.conf`

3. Kopieren Sie "httpd-proxy.conf" zum folgenden Verzeichnis:

   `apacheHome/conf/extra`

4. Öffnen Sie "httpd-proxy.conf", und kommentieren Sie die folgenden Zeilen:

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

5. Navigieren Sie zurück zum Ordner *apache_install_dir**conf*, öffnen Sie "httpd.conf", und entfernen Sie die Kommentarzeichen der folgenden Zeilen (wenn kommentiert):

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

6. Aktualisieren Sie die folgenden Zeilen sowohl in "HTTP Virtual Hosts" als auch in "HTTPS Virtual Hosts", um die Koordinationsrechner-Hostnamen für "BalancerMember" zu ersetzen.

   Ungesicherte Node-Members

   - Knoten 1

     `BalancerMember  http://< Enter node1 hostname>:7000`

- Knoten 2

  ```
  BalancerMember  http://< Enter node2 hostname>:7000
  ```

Gesicherte Node-Members

- Knoten 1

  ```
  BalancerMember  https://< Enter node1 hostname>:7443
  ```

- Knoten 2

  ```
  BalancerMember  https://< Enter node2 hostname>:7443
  ```

7. Ersetzen Sie den Platzhalter "Enter node1 hostname here" (Geben Sie den Hostnamen von Knoten1 hier ein) für "worker.node1.host" mit dem gültigen Wert.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

8. Speichern Sie die Datei httpd-proxy.conf.
9. Öffnen Sie die Datei "apacheHome/conf/httpd.conf", und stellen Sie sicher, dass die Ports 7000 und 7443 nicht verwendet werden.
10. Fügen Sie die folgende Zeile am Ende der Datei "httpd.conf" ein:

    ```
    Include conf/extra/httpd-proxy.conf
    ```

11. Generieren Sie SSL-Zertifikatsdateien, (siehe Seite 51) um "c2okey2.pem"- und "c2ocert.pem"-Dateien zu generieren.
12. Kopieren Sie die generierten Dateien in das Verzeichnis "*apacheHome/*conf".
13. Starten Sie den Apache-Webserver neu.

Konfigurieren der sicheren Konfiguration (Nicht-Windows-Betriebssystem)

In diesem Abschnitt sind Anweisungen für das Installieren und Konfigurieren des Apache-Lastenausgleichs im sicheren Modus enthalten.

Hinweis: Statt Apache können Sie einen anderen Lastenausgleich verwenden. Allerdings ist es für einen CA Process Automation-Koordinationsrechner erforderlich, dass einige Anfrageklassen an einen bestimmten Knoten im geclusterten Koordinationsrechner geleitet werden. Deswegen ist ein einfacher Lastenausgleich nicht ausreichend. Informationen zu Alternativen finden Sie auf der Seite mit den Best Practices für die CA Process Automation-Implementierung, oder kontaktieren Sie den CA Support, um Hilfe zu erhalten. Das Bookshelf enthält Verknüpfungen zu diesen Seiten.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (Nicht-Windows-Betriebssystem) (siehe Seite 279).
2. Konfigurieren Sie die sichere Kommunikation (Nicht-Windows-Betriebssystem) (siehe Seite 284).
3. Apache-Lastenausgleichs-Konfiguration für Catalyst RESTful API (Nicht-Windows-Betriebssystem) (siehe Seite 281)

   Hinweis: Damit der Apache-Webserver HTTPS-Anforderungen an Catalyst-Operatoren weiterleiten kann, müssen die SSL-Zertifikate das PEM-Format aufweisen. Bei Bedarf: Erneutes Generieren von SSL-Zertifikatsdateien (siehe Seite 51).

Konfigurieren der sicheren Kommunikation (Nicht-Windows-Betriebssystem)

Sie können einen Lastenausgleich für sichere Kommunikation konfigurieren. In den folgenden Schritten gibt *certloc* den Speicherort Ihres Zertifikats an.

Gehen Sie folgendermaßen vor:

1. Installieren eines Lastenausgleichs und Vorbereiten der Konfigurationsvorlagen (siehe Seite 268).
2. Öffnen Sie die Datei "workers.properties".
3. Fügen Sie den ersten Knoten hinzu, indem Sie "node1" definieren, das mit der folgenden Zeile beginnt:

   ```
   worker.node1.host=<Enter node1 hostname here>
   ```

4. Ersetzen Sie den Platzhalter *Enter node1 hostname here* von dieser Zeile für "worker.node1.host" mit dem gültigen Wert.

   Hinweis: Gültige Werte sind die IP-Adresse, der FQDN oder der DNS-Alias, der für den Host aufgelöst wird, auf dem Sie den ersten Knoten des Domänen-Koordinationsrechners installieren. Der gültige Wert ist der gleiche Wert, der für "Serverhost" verwendet wird, wenn der Domänen-Koordinationsrechner installiert wird.

5. Speichern und schließen Sie die Datei "workers".
6. Prüfen Sie CA-Standardspeicherorte in der Datai "openssl" im folgenden Verzeichnis.

   apache_install_location/conf

7. Erstellen oder beziehen Sie eine Zertifikatsdatei und eine private Schlüsseldatei mit einem allgemeinen Namen, der mit dem "ServerName" in "httpd.conf" übereinstimmt.

   Zum Beispiel zeigen die folgenden Schritte, wie Sie das im Apache-Lastenausgleich enthaltene Hilfsprogramm "openssl" verwenden sollten, um eine Zertifikatsdatei zu erstellen. Zusätzliche Optionen steuern den Ablauf des Zertifikats, den Dateinamen und die Algorithmen. Sie können sich auf die vom Anbieter bereitgestellte Dokumentation beziehen, wenn Ihr Standort besondere Anforderungen hat.

   a. Öffnen Sie eine Eingabeaufforderung.

   b. Ändern Sie die Verzeichnisse zum Apache-Ordner "bin".

      cd *apache_install_location*/bin

c. Erstellen Sie eine CSR-Datei (Certificate Signing Request) und PEM-Dateien. Geben Sie dafür folgenden Befehl ein, wobei "mypamserver" ein Name Ihrer Wahl ist:

```
openssl req -new -out mypamserver.csr
```

Sie werden aufgefordert, die Passphrase für die PEM-Datei und andere Identifikationsinformationen anzugeben.

- Für die meisten Identifikationsinformationen (Ländernamen, Namen des Bundesstaats/-lands, Namen der Örtlichkeit, Namen der Organisation, Namen der Organisationseinheit) können Sie den Standardwert akzeptieren. Um ein Feld leer zu lassen, geben Sie einen Punkt (.) ein.
- Wenn die Aufforderung für den allgemeinen Namen angezeigt wird, geben Sie als Wert den Teil des Hostnamens von "ServerName" in "*apache_install_location*\conf \httpd.conf" ein.

  Zum Beispiel wenn "ServerName" in httpd.conf den Wert "myhost.mycompany.com:80" hat, geben Sie **myhost.mycompany.com** als allgemeinen Namen an.
- Zu den optionalen Feldern gehören: E-Mail-Adresse, "dir", ein Anfragekennwort und ein optionaler Unternehmensname.

Der Apache-Lastenausgleich erstellt "*mypamserver.*csr" und "*privkey.*pem" im aktuellen Verzeichnis.

d. Erstellen Sie Ihren privaten RSA-Schlüssel. Geben Sie dafür eine Passphrase für "*privkey*.pem" ein, wenn Sie der Apache-Lastenausgleich dazu auffordert.

```
openssl rsa -in privkey.pem -out mypamserver.key
```

e. Erstellen Sie Ihr Zertifikat.

```
openssl x509 -in mypamserver.csr -out mypamserver.cert -req
-signkey mypamserver.key
```

8. Schließen Sie die Eingabeaufforderung, und öffnen Sie Windows Explorer, um generierte Dateien zu kopieren und zu löschen:

   a. Wählen Sie einen "*certloc*"-Ordner aus oder erstellen Sie einen Ordner, um Ihr Zertifikat und die privaten Schlüsseldateien aufzubewahren.

   b. Öffnen Sie den Ordner *apache_install_dir**bin*, wo die Dateien "CERT" und "KEY" generiert wurden.

   c. Ziehen (Verschieben) Sie "*mypamserver*.cert" und "*mypamserver*.key" per Drag-and-drop auf *certloc*.

   d. Löschen Sie die erweiterten Dateien, die im Ordner *apache_install_dir/bin* erstellt wurden. Zu den erweiterten Dateien zählen *mypamserver.CSR*, *privkey.PEM* und ".RND".

9. Sichern Sie die Dateien, die Sie erstellt haben.

10. Ändern Sie mithilfe eines Texteditors die "httpd"-Textdatei ("*apache_install_location*\conf\httpd.conf") folgendermaßen:

    a. Entfernen Sie die Kommentarzeichen am Anfang der folgenden Zeilen:

    ```
    LoadModule rewrite_module modules/mod_rewrite.so

    LoadModule ssl_module modules/mod_ssl.so

    Include conf/extra/httpd-ssl.conf
    ```

    b. Fügen Sie am Ende von "httpd.conf" folgende Zeilen hinzu. Sie können den Text von der Datei "httpd VIRTUALHOST_EXAMPLE" kopieren und einfügen, die Sie aus dem Archiv "SecureDomainConfig_Template.zip" extrahiert haben.

    ```
    <VirtualHost *:80>
    JkMountFile conf/uriworkermap.properties
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
    !^http://.*c2orepository*|MirroringRequestProcessor*|mirror
    ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
    t*
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    </VirtualHost>
    # Load balancing module
    include conf/mod-jk.conf
    ```

    c. Speichern Sie die geänderte "httpd.conf"-Datei, und schließen Sie den Editor.

11. Sichern Sie die Dateien, die Sie bearbeitet haben.

12. Ändern Sie mithilfe eines Texteditors die Konfigurationsdatei *apache_install_location/conf/extra/httpd-ssl.conf* folgendermaßen:

    a. Entfernen Sie das Kommentarzeichen (sofern vorhanden): "Listen 443"

    b. Ändern Sie den "SSLCertificateFile"-Speicherort in ".../*certloc/mypamserver.*cert".

    ```
    SSLCertificateFile "/usr/local/certloc/mypamserver.cert"
    ```

    c. Ändern Sie den "SSLCertificateKeyFile"-Speicherort in ".../*certloc/mypamserver.*key".

    ```
    SSLCertificateKeyFile "/usr/local/certloc/mypamserver.key"
    ```

    d. Fügen Sie die folgenden Zeilen am Ende des <VirtualHost>-Elements hinzu, und zwar vor dem </VirtualHost>-Element:

    ```
    SSLOptions +StdEnvVars +ExportCertData
    JkMountFile conf/uriworkermap.properties
    ```

    e. Speichern Sie die geänderte "httpd.conf-ssl"-Datei, und schließen Sie den Editor.

13. Starten Sie den Apache-Service neu. Klicken Sie dafür im Startmenü auf "Programme", "Apache HTTP Server 2.2", "Control Apache Server" und dann auf "Restart".

    Die Änderungen werden nun wirksam.

Anhang F: Upgrade-Beispiele

Dieses Kapitel enthält folgende Themen:

Beispiel: Upgrade eines Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows (siehe Seite 289)
Beispiel: Upgrade eines weiteren Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows (siehe Seite 296)
Beispiel: Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 unter Windows (siehe Seite 299)
Upgrade von Versionen vor 3.1 SP01 (siehe Seite 305)

Beispiel: Upgrade eines Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows

Das folgende Beispiel ist das erste von zwei verwandten Beispielen für das Upgrade eines geclusterten Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter einem Windows-Betriebssystem. Die Beispiele umfassen Screenshots und Kommentare für das folgende Szenario:

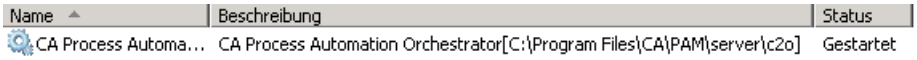
- Domänen-Koordinationsrechner-Knoten 1: pam-sandbox-n1
- Domänen-Koordinationsrechner-Knoten 2: pam-sandbox-n2
- Lastenausgleich für Domänen-Koordinationsrechner: pam-sandbox-LB

Dies sind die Schritte:

1. Melden Sie sich beim Host mit dem Knoten des geclusterten Domänen-Koordinationsrechners an, für den Sie ein Upgrade durchführen möchten.
2. Öffnen Sie die CA Process Automation-Version, für die Sie das Upgrade durchführen. Wählen Sie im Startmenü beispielsweise "Programme", "CA", "CA Process Automation-Domäne 3.1 SP1" aus, und starten Sie die CA Process Automation-Verwaltungskonsole.

   Hinweis: Dies ist eine einfache Methode zum Verifizieren, dass CA EEM ausgeführt wird und Ihr Datenbankserver aktiv ist. Dies ist eine Upgrade-Voraussetzung.

3. Melden Sie sich ab, schließen Sie die CA Process Automation-Verwaltungskonsole, und halten Sie den Koordinationsrechner-Service an. (Wenn Sie "Services" öffnen, können Sie sicherstellen, dass sich der Service nicht im Status "Gestartet" befindet. Fahren Sie nicht fort, solange der Status "Wird angehalten" ist. Aktualisieren Sie diese Ansicht, und warten Sie, bis das Feld "Status" deaktiviert wird.

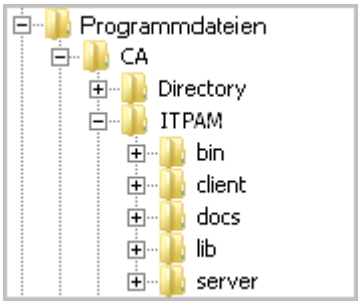


4. Navigieren Sie zum Ordner "DVD1" auf dem Installationsdatenträger, und starten Sie die Datei "Domain_Installer_windows.bat".

5. Klicken Sie auf "Weiter", um die ersten Seiten des Assistenten für das Drittanbieter-Installationsprogramm zu durchlaufen:

   - Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation
   - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung

6. Durchsuchen Sie das System für "Zielverzeichnis auswählen" nach dem exakten Verzeichnis, das die Dateien für CA Process Automation 3.1sp01 enthält: "bin", "client", "docs", "lib" und "server". Dieses Verzeichnis kann den Standardnamen oder einen Namen, den Sie zu einem früheren Zeitpunkt angegeben haben, verwenden.



Wichtig! Sie müssen auf das richtige Verzeichnis verweisen, damit der Installationsprozess Ihre bestehenden Konfigurationsoptionen erkennt.

7. Klicken Sie auf "Weiter", um "Voraussetzungen für die Installation von CA Process Automation" zu durchlaufen.

   Die Installation von Drittanbieterkomponenten startet.

8. Wenn die Seite "JDBC-JAR-Dateien für die Installation" angezeigt wird, klicken Sie auf "Dateien hinzufügen", wenn Sie einen MySQL-Datenbankserver oder SQL Server verwenden. Durchsuchen Sie Ihr System nach dem Speicherort der entsprechenden JAR-Datei.

   Wenn beispielsweise der JDBC-Treiber für SQL Server geändert wurde, durchsuchen Sie Ihr System für SQL Server nach DVD1\drivers\jtds-1.3.jar.

9. Wenn die Seite "Der Setup-Assistent für CA Process Automation wird ausgeführt" angezeigt wird:

   a. Ändern Sie das letzte Verzeichnis des angezeigten Pfads von "DVD1" in "DVD2" um.

Der Setup-Assistent für CA Process Automation wird ausgeführt
Die Installation der Voraussetzungen wurde erfolgreich abgeschlossen.
Legen Sie die CA Process Automation-Installations-DVD ein, oder durchsuchen Sie das System nach dem Speicherort des Inhalts des CA Process Automation-Installationsprogramms. Klicken Sie auf 'Fertig stellen', um die CA Process Automation-Installation zu starten.
Domäne verwenden
Verzeichnis
:\Administrator\Desktop\14th november\DVD2\
Durch...

   b. Klicken Sie auf "Fertig stellen".

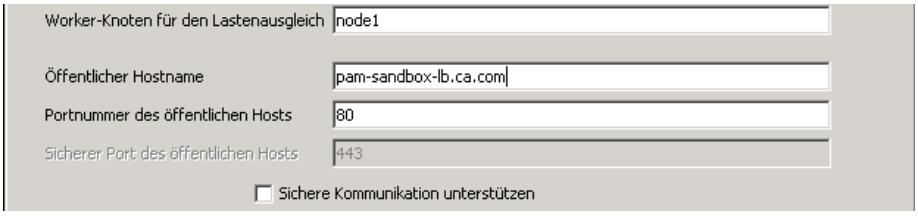
      Es wird folgende Nachricht angezeigt: "Das CA Process Automation-Installationsprogramm wird kopiert. Dies kann einige Minuten dauern, bitte warten Sie."

10. Wenn "Willkommen beim Setup-Assistenten für CA Process Automation-Domäne" angezeigt wird, klicken Sie sich durch die ersten Seiten des Assistenten:

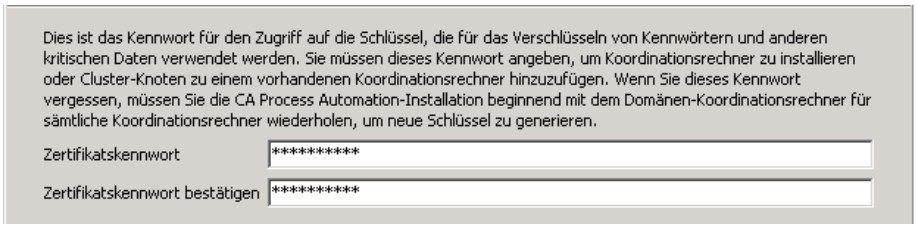
    - Sprache
    - Willkommen beim Setup-Assistenten für CA Process Automation-Domäne
    - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung.
    - Java-Home-Verzeichnis: Dies wird automatisch ausgewählt, zum Beispiel C:\Programme\Java\jdk1.7.0_x.
    - Neu installieren/Konfigurieren: Die Optionsmittel "Neu installieren" bedeutet **Upgrade**.

      Die Nachricht "Die gesamte Konfiguration wird kopiert" wird angezeigt.
    - Konfigurationsbildschirm

      Im folgenden Beispiel werden unsere Beispieldaten verwendet:

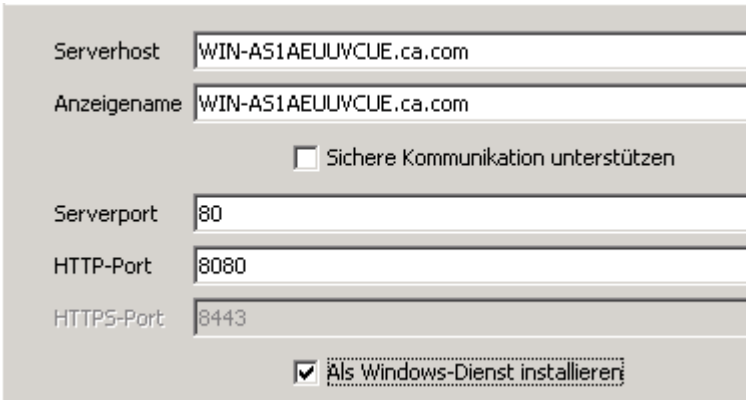


11. Wenn "Zertifikatskennwort festlegen" angezeigt wird, geben Sie *dasselbe* Zertifikatskennwort ein, das in der Vorgängerversion verwendet wurde, und klicken Sie auf "Weiter".


Dies ist das Kennwort für den Zugriff auf die Schlüssel, die für das Verschlüsseln von Kennwörtern und anderen kritischen Daten verwendet werden. Sie müssen dieses Kennwort angeben, um Koordinationsrechner zu installieren oder Cluster-Knoten zu einem vorhandenen Koordinationsrechner hinzuzufügen. Wenn Sie dieses Kennwort vergessen, müssen Sie die CA Process Automation-Installation beginnend mit dem Domänen-Koordinationsrechner für sämtliche Koordinationsrechner wiederholen, um neue Schlüssel zu generieren.
Zertifikatskennwort
****
Zertifikatskennwort bestätigen
****

12. Klicken Sie auf "Weiter", um den Startmenüordner auszuwählen. Standardmäßig wird "CA Process Automation 4.2" verwendet.
13. Klicken Sie in "Allgemeine Eigenschaften" auf "Weiter". "Als Windows-Dienst installieren" ist standardmäßig aktiviert.

    Im folgenden Beispiel werden unsere Beispieldaten verwendet:

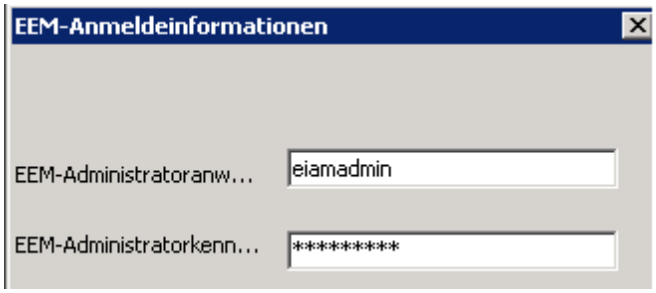


14. Klicken Sie auf "Weiter", um die folgenden Seiten zu durchlaufen:
    - Temporäres Skriptenverzeichnis
    - Richtlinie für PowerShell-Ausführung
15. Wenn die Sicherheitseinstellungen für Embedded Entitlements Manager (EEM) angezeigt werden, werden standardmäßig die Eingaben Ihrer bestehenden Konfiguration verwendet. Zum Beispiel:

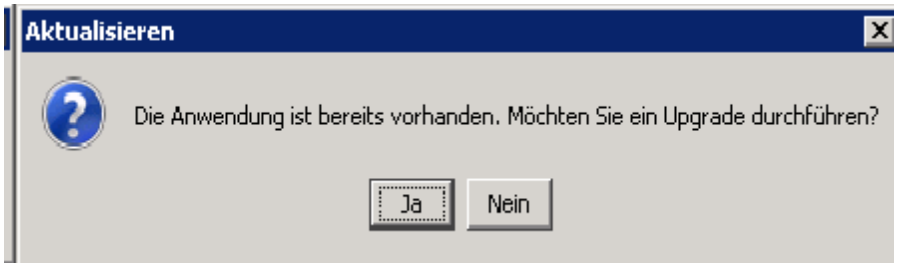
a. Überspringen Sie das Feld "Standardmäßige Active Directory-Domäne", außer, Sie haben CA EEM für die Verwendung mehrerer Microsoft Active Directory-Verzeichnisse konfiguriert. Geben Sie in diesem Fall den Namen eines der AD-Verzeichnisse, die Sie konfiguriert haben, ein.

b. Wählen Sie "Anwendung mit CA EEM registrieren" aus, und klicken Sie auf "Registrieren".

c. Geben Sie Anmeldeinformationen für die Anmeldung bei CA EEM als EiamAdmin-Administrator an, und klicken Sie auf "OK".



d. Klicken Sie auf "Ja", um dem Upgrade zuzustimmen.

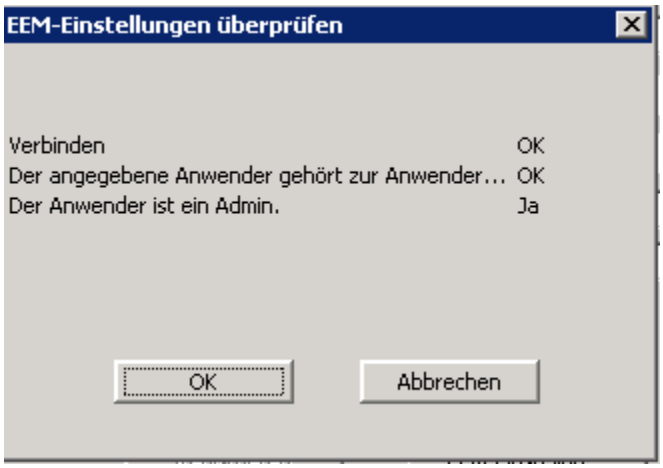


e. Klicken Sie in der Nachricht "Upgrade für die Anwendung durchgeführt" auf "OK".

f. (Optional). Klicken Sie auf "EEM-Einstellungen testen", und füllen Sie "EEM-Einstellungen überprüfen" aus:

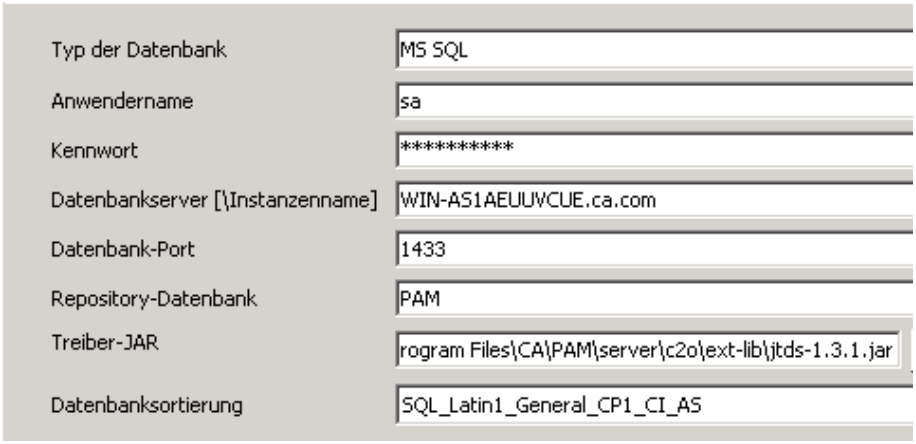
   - Wenn Ihre Anwender-Anmeldeinformationen in CA EEM gespeichert werden, geben Sie den Anwendernamen und das Kennwort für Ihr CA Process Automation-Anwenderkonto ein.
   - Wenn CA EEM Active Directory verwendet, geben Sie Ihre AD-Anmeldeinformationen ein.

   Reagieren Sie auf die Bestätigungsmeldung.



16. Wenn die folgenden Datenbankeinstellungen angezeigt werden, klicken Sie auf "Datenbankeinstellungen testen", um zu überprüfen, ob "Test erfolgreich abgeschlossen" angezeigt wird. Klicken Sie auf "Weiter".
    - Repository-Datenbank (auch als Bibliotheksdatenbank bezeichnet)
    - Laufzeitdatenbank
    - Berichtsdatenbank

    Im folgenden Beispiel werden unsere Beispieldaten verwendet:



17. Klicken Sie in "Zusätzliche JAR-Dateien für Installation" auf "Weiter", bzw. treffen Sie bei Bedarf eine Auswahl aus der angezeigten Liste, um zusätzliche Dateien hinzuzufügen.
18. Warten Sie, während Setup ein Upgrade (eine Installation) der CA Process Automation-Domäne durchführt.
19. Wenn "Der Setup-Assistent für CA Process Automation-Domäne wird ausgeführt" angezeigt wird, klicken Sie auf "Fertig stellen".
20. Melden Sie sich vom Server, auf dem das Upgrade für Knoten 1 des geclusterten Domänen-Koordinationsrechners durchgeführt wurde, ab.

Hinweis: Wenn Connectors aktualisiert werden müssen, starten Sie den Koordinationsrechner-Service erst, wenn diese Aktualisierung abgeschlossen ist.

Beispiel: Upgrade eines weiteren Knotens des Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter Windows

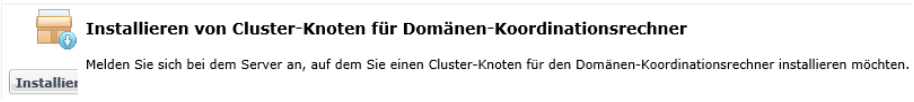
Das folgende Beispiel ist das zweite von zwei verwandten Beispielen für das Upgrade eines geclusterten Domänen-Koordinationsrechners von 3.1 SP01 auf Version 4.2 unter einem Windows-Betriebssystem. Die Beispiele umfassen Screenshots und Kommentare für das folgende Szenario:

- Domänen-Koordinationsrechner-Knoten 1: pam-sandbox-n1
- Domänen-Koordinationsrechner-Knoten 2: pam-sandbox-n2
- Lastenausgleich für Domänen-Koordinationsrechner: pam-sandbox-LB

Dies sind die Schritte:

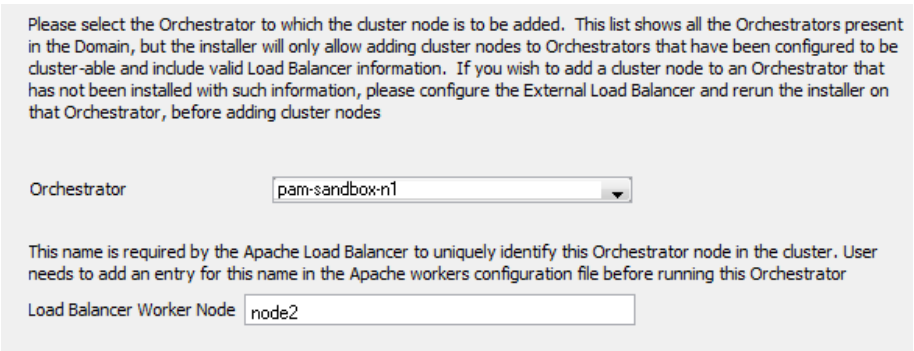
1. Melden Sie sich bei dem Server an, für den Sie das erste Upgrade durchgeführt haben. Starten Sie den Koordinationsrechner-Service über "Verwaltung", "Dienste". Beachten Sie, dass der Pfad derselbe ist, unter dem Sie CA Process Automation anfänglich installiert haben.

2. Melden Sie sich bei einem Server, auf dem ein anderer Knoten (zum Beispiel node2) des geclusterten Domänen-Koordinationsrechner installiert ist, an.
3. Navigieren Sie zur URL der Domäne, dem Lastenausgleich für den Domänen-Koordinationsrechner. In diesem Beispiel ist dies http://pam-sandbox-lb/itpam.
4. Melden Sie sich an, klicken Sie auf die Registerkarte "Konfiguration", und klicken Sie anschließend unten links auf das Auswahlmenü "Installation".
5. Klicken Sie unter "Installieren von Cluster-Knoten für Domänen-Koordinationsrechner" auf "Installieren", um das Upgrade zu starten.

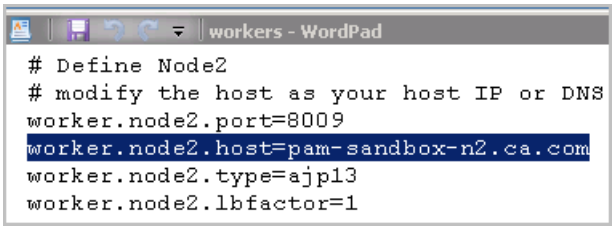

Installieren von Cluster-Knoten für Domänen-Koordinationsrechner
Melden Sie sich bei dem Server an, auf dem Sie einen Cluster-Knoten für den Domänen-Koordinationsrechner installieren möchten.
Installier

6. Als Erstes wird das Dialogfeld für die Sprachauswahl angezeigt. Klicken Sie auf OK.
7. Klicken Sie sich durch die folgenden Seiten des Assistenten:
   - Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation.
   - Lizenzvereinbarung: Wählen Sie "Ich akzeptiere die Bedingungen der Lizenzvereinbarung" aus
   - Zielverzeichnis auswählen: Standardmäßig C:\Programme\CA\PAM.
   - Voraussetzungen für die Installation von CA Process Automation: Ruft die Installation auf.
   - "Der Setup-Assistent für CA Process Automation wird ausgeführt" (mit "Domäne verwenden" aktiviert): Klicken Sie auf "Fertig stellen"

     Warten Sie, bis die nächste Seite angezeigt wird. Der Fortschritt der Verarbeitung bis zur Anzeige der nächsten Seite wird nicht durch einen visuellen Indikator angezeigt.
   - Willkommen beim Setup-Assistenten für CA Process Automation-Domäne
   - License Agreement (Lizenzvereinbarung)
8. Wenn Sie ein Upgrade Ihres JDK durchgeführt haben, durchsuchen Sie Ihr System nach dem zum Java-Home-Verzeichnis, beispielsweise C:\Programme\Java\jdk1.7.0_45
9. Wenn der Konfigurationsbildschirm angezeigt wird:
   a. Klicken Sie auf die Drop-down-Liste "Koordinationsrechner", und wählen Sie den Knoten des Domänen-Koordinationsrechners aus, für den Sie als Erstes ein Upgrade durchgeführt haben.

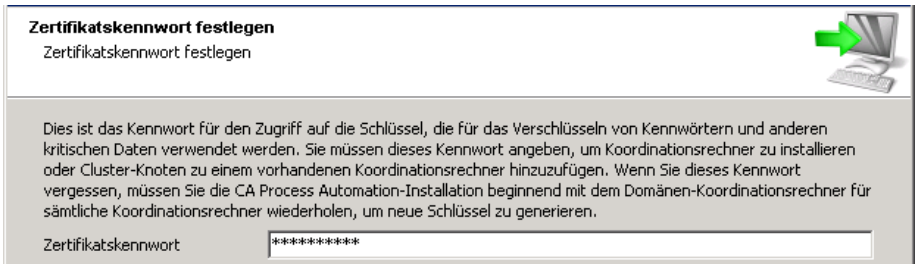

Please select the Orchestrator to which the cluster node is to be added. This list shows all the Orchestrators present in the Domain, but the installer will only allow adding cluster nodes to Orchestrators that have been configured to be cluster-able and include valid Load Balancer information. If you wish to add a cluster node to an Orchestrator that has not been installed with such information, please configure the External Load Balancer and rerun the installer on that Orchestrator, before adding cluster nodes
Orchestrator
pam-sandbox-n1
This name is required by the Apache Load Balancer to uniquely identify this Orchestrator node in the cluster. User needs to add an entry for this name in the Apache workers configuration file before running this Orchestrator
Load Balancer Worker Node
node2

b. Geben Sie im Feld "Worker-Knoten für den Lastenausgleich" einen Wert ein. Tippen Sie den Kennzeichner für den Knoten, auf dem Sie das Upgrade durchführen (node2, node3, node4), ein. Verwenden Sie das Format worker.**node2**.host=*aktueller-Host*, das in der Datei "workers.properties" im Ordner *Apache_Installationsverzeichnis/conf* definiert wurde.



In diesem Beispiel wurde als Wert für worker.**node2**.host=pam-sandbox-n2 in "workers.properties" node2 des Domänen-Koordinationsrechner-Cluster definiert. Das Feld "Öffentlicher Hostname" wird automatisch mit dem FQDN des Lastenausgleichs aufgefüllt.

10. Geben Sie den Namen Ihres Unternehmens ein.
11. Tippen Sie *dasselbe* Zertifikatskennwort ein, das Sie bei der Installation des vorigen Knotens des Domänen-Koordinationsrechners eingegeben haben. Dies ist *dasselbe* Zertifikatskennwort, das in der Vorgängerversion vom Domänen-Koordinationsrechner verwendet wurde.


Zertifikatskennwort festlegen
Zertifikatskennwort festlegen
Dies ist das Kennwort für den Zugriff auf die Schlüssel, die für das Verschlüsseln von Kennwörtern und anderen kritischen Daten verwendet werden. Sie müssen dieses Kennwort angeben, um Koordinationsrechner zu installieren oder Cluster-Knoten zu einem vorhandenen Koordinationsrechner hinzuzufügen. Wenn Sie dieses Kennwort vergessen, müssen Sie die CA Process Automation-Installation beginnend mit dem Domänen-Koordinationsrechner für sämtliche Koordinationsrechner wiederholen, um neue Schlüssel zu generieren.
Zertifikatskennwort
****

12. Klicken Sie sich durch die folgenden Seiten. In diesem Beispiel werden die Einstellungen von node1 verwendet.
    - Auswahl des Startmenüordners.
    - Seite "Allgemeine Eigenschaften" ("Als Windows-Dienst installieren" wird nicht angezeigt, sondern als Standard verwendet).
    - Temporäres Skriptenverzeichnis
    - PowerShell
    - CA Embedded Entitlements Manager CA EEM-Sicherheitseinstellungen
    - Datenbankeinstellungen - Repository
    - Datenbankeinstellungen - Laufzeit
    - Datenbankeinstellungen - Berichterstellung

    Die Upgrade-Installation wird gestartet.
13. Wenn die Seite "Der Setup-Assistent für CA Process Automation-Domäne wird ausgeführt" angezeigt wird, klicken Sie auf "Fertig stellen".

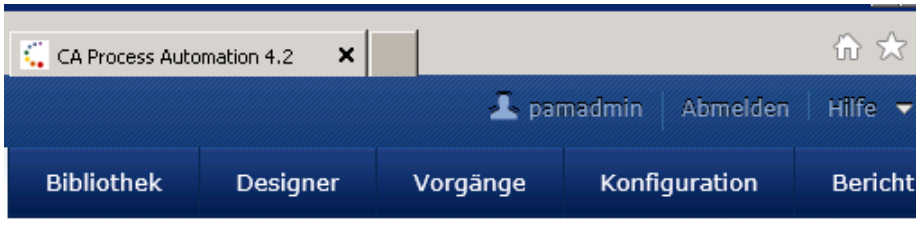
Beispiel: Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 unter Windows

Das folgende Beispiel enthält ausgewählte Screenshots, die jenen ähneln, die angezeigt werden, wenn Sie unter einem Windows-Betriebssystem ein Upgrade eines nicht geclusterten Koordinationsrechners von 4.1 SP01 auf Version 4.2 durchführen. Wenn Sie mit dem CA Process Automation-Installationsassistenten nicht vertraut sind, kann dies hilfreich sein.

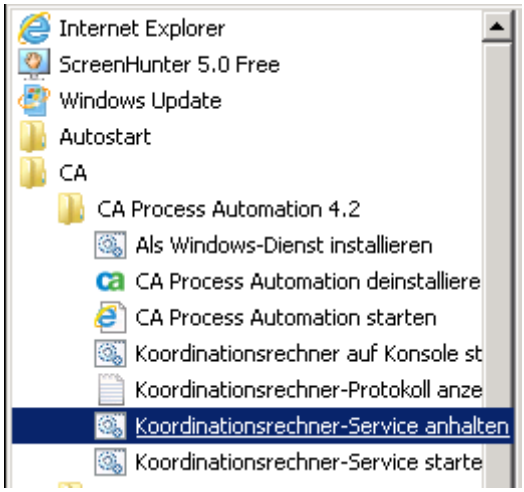
Dies sind die Schritte:

1. Melden Sie sich bei dem Host an, auf dem der Domänen-Koordinationsrechner konfiguriert ist.
2. Öffnen Sie die CA Process Automation-Version, für die Sie das Upgrade durchführen. Wählen Sie im Startmenü "CA", "CA Process Automation 4.1 SP01" und "CA Process Automation starten" aus.

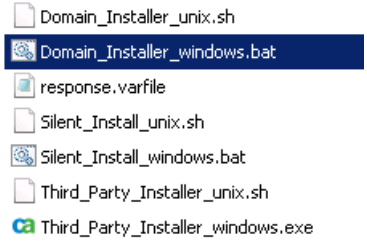
   Hinweis: Dies ist eine einfache Methode zum Verifizieren, dass CA EEM ausgeführt wird und Ihr Datenbankserver aktiv ist. Dies ist eine Upgrade-Voraussetzung.



3. Melden Sie sich von CA Process Automation ab, schließen Sie den Browser, und halten Sie den Koordinationsrechner-Service an. Wählen Sie dafür beispielsweise im Startmenü "CA", "CA Process Automation 4.1 SP01" und "Koordinationsrechner-Service anhalten" aus. (Wenn Sie "Services" öffnen, können Sie sicherstellen, dass sich der Service nicht im Status "Gestartet" befindet.)



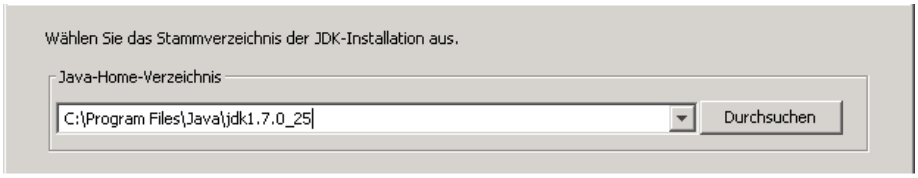
4. Navigieren Sie zum Ordner "DVD1" auf dem Installationsdatenträger, und starten Sie die Datei "Domain_Installer_windows.bat".



5. Klicken Sie auf "Weiter", um die ersten Seiten des Assistenten zu durchlaufen:
   - Sprache
   - Willkommen beim Assistenten für das Drittanbieter-Installationsprogramm von CA Process Automation
   - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung
   - Zielverzeichnis auswählen
   - Voraussetzungen für die Installation von CA Process Automation

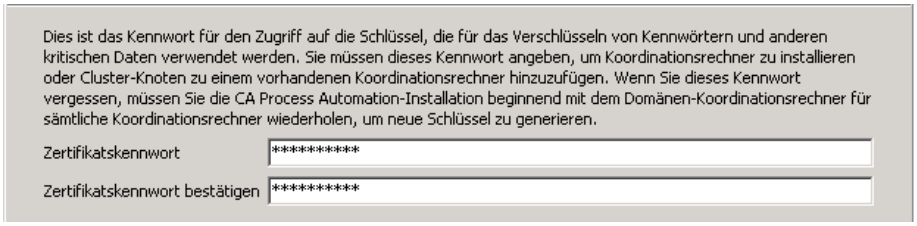
     Die Installation startet. Active MQ und Drittanbieterkomponenten werden dabei ebenfalls installiert.
   - Installation von JDBC-JAR-Dateien (standardmäßig werden die JDBC-JAR-Dateien verwendet, die beim Upgrade des Domänen-Koordinationsrechners angegeben wurden.)
   - Voraussetzungen für die Installation von CA Process Automation (erfolgreich abgeschlossen)
6. Wenn "Der Setup-Assistent für CA Process Automation wird ausgeführt" angezeigt wird, ersetzen Sie "DVD1" im Verzeichnispfad durch "DVD2". Klicken Sie anschließend auf "Fertig stellen".

   Die folgende Nachricht wird angezeigt: "Das CA Process Automation-Installationsprogramm wird kopiert. Dies kann einige Minuten dauern, bitte warten Sie". Zwischen dem Schließen dieser Seite und dem Öffnen der Seite "Willkommen" kann etwas Zeit vergehen.
7. Wenn "Willkommen beim Setup-Assistenten für CA Process Automation-Domäne" angezeigt wird, klicken Sie sich durch die ersten Seiten des Assistenten:
   - Sprache
   - Willkommen beim Setup-Assistenten für CA Process Automation-Domäne
   - Lizenzvereinbarung: Ich akzeptiere die Bedingungen der Lizenzvereinbarung
8. Durchsuchen Sie Ihr System unter "CA Process Automation-Domäne", "Legen Sie das Java-Home-Verzeichnis fest" nach dem korrekten Verzeichnis.



9. Fahren Sie fort, sich durch die Seiten zu klicken:
   - CA Process Automation-Domäne, Neu installieren/Konfigurieren: Für Upgrades ist nur die Option "Neu installieren" verfügbar.
   - CA Process Automation-Domäne, Konfigurationsbildschirm

10. Wenn "Zertifikatskennwort festlegen" angezeigt wird, geben Sie *dasselbe* Zertifikatskennwort ein, das vom Domänen-Koordinationsrechner verwendet wird. Dieses Zertifikatskennwort muss mit jenem Kennwort übereinstimmen, das bei der anfänglichen Installation dieses nicht geclusterten Koordinationsrechners angegeben wurde. Klicken Sie auf "Weiter".


Dies ist das Kennwort für den Zugriff auf die Schlüssel, die für das Verschlüsseln von Kennwörtern und anderen kritischen Daten verwendet werden. Sie müssen dieses Kennwort angeben, um Koordinationsrechner zu installieren oder Cluster-Knoten zu einem vorhandenen Koordinationsrechner hinzuzufügen. Wenn Sie dieses Kennwort vergessen, müssen Sie die CA Process Automation-Installation beginnend mit dem Domänen-Koordinationsrechner für sämtliche Koordinationsrechner wiederholen, um neue Schlüssel zu generieren.
Zertifikatskennwort
****
Zertifikatskennwort bestätigen
****

11. Klicken Sie sich durch Seite zum Auswählen des Startmenüordners, um Ihre bestehende Auswahl zu verwenden.

12. Beachten Sie auf der Seite "Allgemeine Eigenschaften" die folgenden Änderungen an den Standardwerten für den Koordinationsrechner-Serverport:

    Serverport

    Gibt den Port an, den der Domänen-Koordinationsrechner verwendet, um mit anderen Koordinationsrechnern und Agenten zu kommunizieren.

    Standard: 80 (Basis: HTTP) oder 443 (Gesichert: HTTPS)

    Veralteter Serverport

    (Nur für Upgrade/Neuinstallation) Der Wert "Serverport", der für eine vorherige Version von CA Process Automation angegeben wurde.

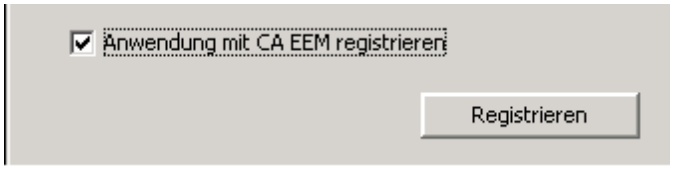
    Standard: 7001

13. Klicken Sie sich durch die folgenden Seiten. Nehmen Sie dabei bei Bedarf Änderungen vor.

    - Temporäres Skriptenverzeichnis
    - Richtlinie für PowerShell-Ausführung

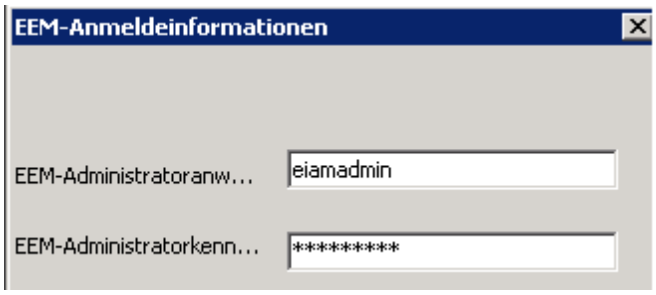
14. Wenn die Sicherheitseinstellungen für Embedded Entitlements Manager (EEM) angezeigt werden:

    a. Wählen Sie "Anwendung mit CA EEM registrieren" aus, und klicken Sie auf "Registrieren". Dies ist bei Upgrades immer ein sinnvoller Schritt, da neue Versionen möglicherweise Änderungen oder Ergänzungen an CA EEM-Richtlinien für CA Process Automation enthalten. Wenn zwischen Versionen keine Änderungen vorgenommen wurden, werden Sie in einet Meldung benachrichtigt, dass kein Upgrade erforderlich ist.

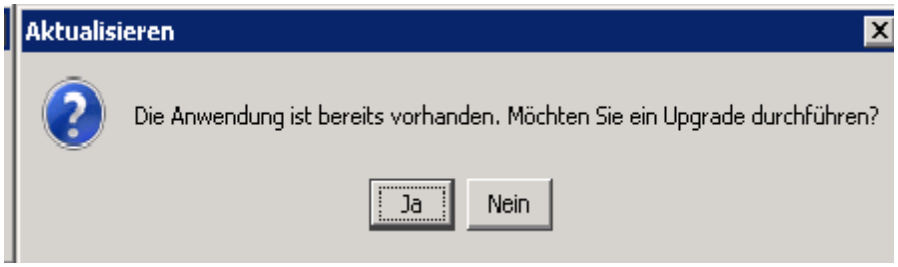


b. Wenn Sie versuchen, diese Seite ohne Registrierung zu verlassen, und der Installationsprozess ein Upgrade der CA Process Automation-Version entdeckt, werden Sie vom Installationsprozess aufgefordert, "Anwendung mit CA EEM registrieren" auszuwählen und anschließend auf "Registrieren" zu klicken.

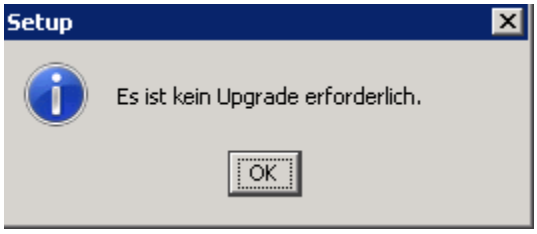
c. Geben Sie Anmeldeinformationen für die Anmeldung bei CA EEM als EiamAdmin-Administrator an.



d. Akzeptieren Sie die Durchführung des Upgrade. Der Installationsprozess ermittelt die Version des CA EEM-Servers und wählt den passenden SDK aus.



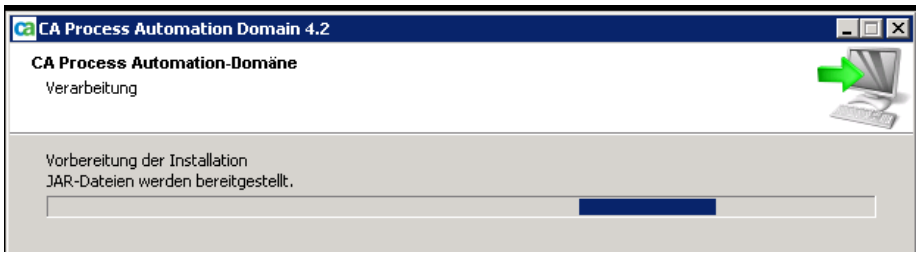
e. Wenn kein Upgrade erforderlich ist, wird die folgende Meldung angezeigt:



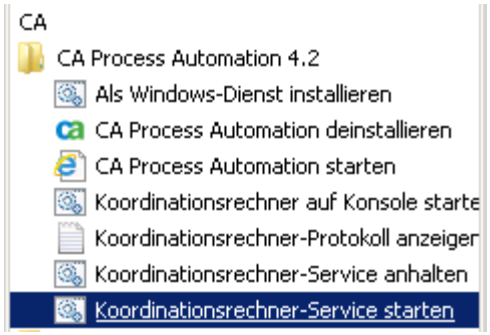
f. Wenn die Bestätigung "Anwendung registriert" angezeigt wird, klicken Sie auf "OK".

15. Klicken Sie sich durch die Datenbankeinstellungen, die Sie bereits definiert haben:
    - Repository-Datenbank
    - Laufzeitdatenbank
    - Berichtsdatenbank
16. Wenn nichts hinzugefügt werden muss, klicken Sie sich durch "Zusätzliche JAR-Dateien für Installation".

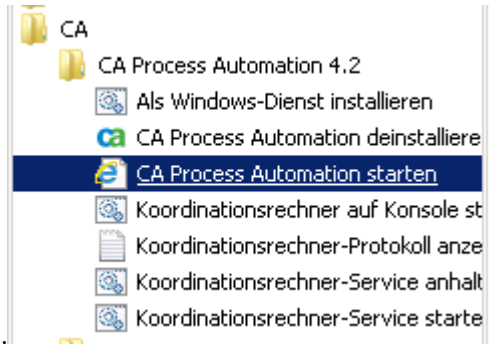
    Setup führt ein Upgrade (eine Installation) der CA Process Automation-Domäne durch.



17. Wenn "Der Setup-Assistent für CA Process Automation-Domäne wird ausgeführt" angezeigt wird, klicken Sie auf "Fertig stellen". Warten Sie den Abschluss der Schemaaktualisierungen ab, bevor Sie versuchen, CA Process Automation zu starten.
18. Starten Sie den Koordinationsrechner-Service.



19. Starten Sie CA Process Automation.



Upgrade von Versionen vor 3.1 SP01

Sie können kein direktes Upgrade von Version 2.x, 3.0 oder 3.0sp01 von CA IT Process Automation Manager (CA IT PAM) auf Version 4.2 von CA Process Automation durchführen. Sie müssen zuerst ein Übergangs-Upgrade durchführen.

Gehen Sie folgendermaßen vor:

1. Führen Sie ein Upgrade von einer älteren Version auf CA Process Automation 3.1 SP01 durch.
   - CA IT PAM Release 2.x
   - CA IT PAM Version 3
   - CA IT PAM Service Pack 3.0 SP01

   Hinweis: Informationen zu diesem Übergangs-Upgrade finden Sie im entsprechenden Installationshandbuch, das Sie vom Kunden-Support herunterladen können.
2. Führen Sie das Upgrade von CA Process Automation Service Pack 3.1 SP01 auf Version 4.2 von CA Process Automation durch. Die entsprechende Beschreibung finden Sie unter So führen Sie ein Upgrade von CA Process Automation durch (siehe Seite 146).